UNIVERSIDAD NACIONAL DE PIURA
OPTO. ADQUISICIONES
BIBLIOTECA CENTRAL

UNIVERSIDAD NACIONAL DE PIURA

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRONICA

TESIS PARA OPTAR EL TÍTULO DE:

Ingeniero Electrónico y Telecomunicaciones

"ESTUDIO DE LOS DIFERENTES MODELOS DE INTER-AS MPLS-VPNs PARA BRINDAR UNA PROPUESTA TÉCNICA QUE PERMITA LA COMUNICACIÓN ENTRE MÚLTIPLES PROVEEDORES DE SERVICIOS"

Presentado por:

Br. Jorge Luis Santamaría Silupu

Br. Iván Eduardo Oviedo Calle

Asesorado por:

Dr. Carlos Enrique Arellano Ramírez

Piura, 2016

7758
SAN

UNIVERSIDAD NACIONAL DE PIURA
OPTO. ADQUISICIONES
BIBLIOTECA CENTRAL

TITULO DEL PROYECTO

"ESTUDIO DE LOS DIFERENTES MODELOS DE INTER-AS MPLS-VPNs PARA BRINDAR UNA PROPUESTA TÉCNICA QUE PERMITA LA COMUNICACIÓN ENTRE MÚLTIPLES PROVEEDORES DE SERVICIOS"

RESPONSABLES DEL DESARROLLO DE LA TESIS

BACH. IVAN EDUARDO OVIEDO CALLE

BACH. JORGE LUIS SANTAMARIA SILUPU

ASESOR. DR. CARLOS ENRIQUE ARELLANO RAMÍREZ

JURADO EVALUADOR

ING. AYAX MANUEL SIFUENTES MONTES

PRESIDENTE

ING. MARIO AUGUSTO RAMOS ECHEVARRIA

SECRETARIO

ING. EDUARDO OMAR AVILA REGALADO

VOCAL

UNIVERSIDAD NACIONAL DE PIURA
DPTO. ADQUISICIONES
BIBLIOTECA CENTRAL

DEDICATORIA

Es deseo mutuo dedicar esta
tesis primero a dios
como tutor de nuestras
vidas, a nuestros padres,
quienes han sido, son y serán
pilares fundamentales en
cada paso de nuestras vidas y
a todas las personas que nos
han brindado su apoyo en el
transcurso del desarrollo
de nuestra tesis de
grado.

AGRADECIMIENTO

A nuestras familias por el apoyo incondicional que siempre nos dieron. Externamos el más sincero y eterno agradecimiento por ese apoyo que perpetuamente nos han brindado y gracias al cual hemos logrado terminar nuestra carrera profesional, que es para nosotros la mejor de las herencias.

A nuestros maestros que día a día forjaron en nosotros las habilidades y actitudes que nos permitieron desarrollar nuestra tesis.

Al ingeniero Carlos Enrique Arellano Ramírez, por aceptar ser nuestro asesor y por su ayuda con las correcciones y planteamientos de la Tesis.

Con un infinitito agradecimiento a nuestra querida Universidad Nacional de Piura por permitirnos vivir una de nuestras mejores etapas de nuestra vida; con especial agradecimiento a nuestra Facultad de Ciencias la cual nos ha dado las herramientas que nos servirán tanto en el ámbito profesional como académico.

RESUMÉN

El propósito de este trabajo de tesis es ofrecer una propuesta técnica que permita la comunicación de una red MPLS-VPNs entre múltiples proveedores de servicios. Durante el desarrollo de esta tesis se presenta el marco teórico de las redes MPLS – VPNs y se realiza un estudio del desempeño de cada uno los diferentes modelos de red para la implementación de las Inter-as MPLS-VPNS con el objetivo de observar las ventajas, desventajas, problemas y las posibles soluciones que ofrece cada modelo.

Para el diseño de cada modelo de implantación nos ayudamos del programa de simulación "GNS3", con equipos de la marca Cisco (Modelos 7600 y 3725). Los procesos realizados en entornos reales pueden ser simulados, garantizando que el funcionamiento de la red sea el esperado al momento de implementarlo en los dispositivos reales. La Plataforma GNS3 es una herramienta muy poderosa y brinda la capacidad de realizar pruebas rigurosas, que en una red real, pueda afectar el rendimiento de los equipos provocando caídas de servicios y pérdidas económicas para la empresa.

Luego, se presenta la propuesta técnica para la implementación de la red, utilizando el modelo que genera los mejores resultados y que garantiza la escalabilidad y calidad de servicio que las empresas requieren para sus VPNs.

Por último, se detallan las conclusiones logradas luego de desarrollar esta tesis y se muestran las futuras líneas de trabajo que han surgido por medio del trabajo realizado.

Palabras Claves: MPLS, VPN, Inter-AS MPLS VPN, ETIQUETA.

ABSTRACT

The purpose of this thesis is to provide a technical proposal to allow communication of MPLS-VPNs among multiple providers. During the development of this thesis the theoretical framework of -VPNs MPLS networks is presented and a study is made of the performance of each different network models for the implementation of the Inter-AS MPLS-VPNS order to see the advantages , disadvantages, problems and possible solutions offered by each model.

For the design of each model we help implement simulation program "GNS3" with the Cisco brand equipment (Models 7600 and 3725). The processes performed in real environments can be simulated, ensuring that the network performance is expected when deploying to actual devices. The GNS3 Platform is a very powerful tool and provides the ability to perform rigorous testing in a real network that might affect the performance of equipment and services falls causing economic losses for the company.

Then the technical proposal for the implementation of the network is presented, using the model generates the best results and ensuring scalability and service quality that companies require for their VPNs.

Finally, the conclusions reached after developing this thesis and future lines of work that have emerged through the work done is detailed.

Keywords: MPLS, VPN, MPLS VPN Inter-AS, TAG.

INDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

1.1 Enunciado del Problema

Las empresas de servicios de telecomunicaciones en nuestro país, buscan ampliar los alcances de sus redes MPLS como tecnología WAN. El Multi-Protocol Label Switching (MPLS) proporciona alta capacidad para integrar voz, vídeo y datos en una plataforma común con garantías de calidad de servicio (QoS), por lo que es muy usada para implementar redes privadas virtuales o VPNs, que hacen posible la integración de los datos de un punto hacia otro usando la gran nube de internet existente. Pero el uso de esta tecnología implica que los clientes de servicios VPN estén conectados a un solo proveedor.

En un mundo en el que día a día las empresas tienden a incursionar en nuevos mercados, en busca de más y más clientes de diferentes ciudades, y realidades sociales, se hace necesaria la comunicación dentro de sus diferentes sedes para transmitir información sobre ventas o estrategias de negocio, para informar sobre la producción minuto a minuto, o cualquier otro fin; este tipo de crecimiento empresarial ha dado lugar a la utilización de los servicios VPN para interconectar sus sedes.

Es por ello que las VPNs de estas empresas necesitarían abarcar grandes áreas geográficas, muchas veces cruzando más de un país, lo que implicaría atravesar redes de múltiples proveedores de servicios VPN. Esto ha creado la necesidad de contar con una solución que permita brindar de forma eficiente servicios VPN altamente escalable, que abarque grandes aéreas geográficas y que sea capaz de integrar a más de un proveedor.

Muchos proveedores de servicios que han implementado MPLS-VPNs por años ahora se enfocan a la interconexión de su red con las redes MPLS-VPN de otros proveedores para así mejorar la escalabilidad y facilidad de operación de su red. Esto implica que muchas veces existirán VPNs que deban abarcar más de un sistema autónomo. Es ante esta problemática que las INTER-AS MPLS-VPNs aparecen como la solución y a la cual nos conlleva a realizar un estudio del desempeño de los diferentes modelos de Inter-AS MPLS-VPNS.

La importancia de la solución de este inconveniente se basa principalmente en la poca documentación que existe en español sobre la implementación de una red MPLS-VPN sobre múltiples sistemas autónomos, que hoy en día está presente en la mayoría de las redes de comunicaciones de gran escala. En esta tesis se desarrollará un estudio del desempeño de diferentes modelos de implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos, el cual busca explicar con modelos de red y conceptos claros y comprensibles, las ventajas y desventajas de cada solución mediante la implementación de cada modelo red con el uso de herramientas muy poderosas como el simulador GNS3, que permitirá analizar los datos de una red tal y como se trabajara en un entorno real con equipos de plataforma Cisco y que además ayudará a identificar la mejor alternativa para la elaboración de una propuesta técnica para su implementación con equipos reales que garantice la escalabilidad y facilidad de operación de la red que las grandes empresas requieren en sus redes privadas virtuales o VPNs.

1.2 Justificación e importancia de la investigación

Del punto de vista tecnológico, los servicios VPN han tenido un crecimiento constante tanto en el Perú como en el mundo. En Latinoamérica el Perú es el cuarto país en número de servicios VPN y en número de clientes. Ante esta tendencia, se hace necesaria la implementación de redes capaces de soportar el aumento sostenido de clientes. Además, la ingeniería de tráfico y la precisión e inteligencia del encaminamiento basado en MPLS permiten empaquetar más datos en el ancho de banda disponible y reducir los requerimientos de procesamiento a nivel de router.

Esta creciente necesidad de reducir costes, aumentar la productividad, soportar más aplicaciones y elevar la seguridad está jugando fuerte a favor del cambio corporativo hacia esta nueva tecnología WAN.

Del punto de vista personal, queremos ampliar nuestros conocimientos en esta tecnología WAN, y conocer sus principales aplicaciones como función de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente), PolicyRouting, Servicios de VPN y Servicios que requieren QoS y a la vez ir a la exigencia y competitividad laboral que hoy en día demandan las empresas.

1.3 Objetivos

1.3.1 Objetivo general

El objetivo de la presente tesis es realizar un estudio y análisis de los diferentes modelos de INTER-AS MPLS-VPNS con el fin de brindar una propuesta técnica para la implementación de una red MPLS-VPN que permita la comunicación entre múltiples proveedores de servicios.

1.3.2 Objetivos específicos

- Explicar de una manera concisa y práctica la tecnología MPLS y su funcionamiento.
- Revisar los conceptos teóricos de los procesos globales (enrutamiento, reenvío) utilizados en una red sobre la que corre MPLS.
- Diseñar y simular topologías que sirvan para explicar el funcionamiento de los procesos básicos MPLS y VPN que, permitan corroborar el funcionamiento de la tecnología en casos reales.
- Comprender la necesidad de utilizar redes MPLS-VPN sobre Múltiples Sistemas Autónomos para brindar servicios de redes privadas virtuales a clientes corporativos.
- Se buscará la mejor alternativa y se elaborará una propuesta técnica que garantice la escalabilidad y calidad de servicio que el sector corporativo requiera para sus redes privadas virtuales o VPNs.

1.4 Estructura de la tesis

Con base al objetivo de este documento, a continuación se describe como ha sido organizada esta tesis, incluyendo una breve descripción de lo que se presenta en cada capítulo.

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA: En este capítulo se especifican los fundamentos de la tesis y los objetivos, que de manera general dan una visión de lo que se pretende con la realización de esta tesis y hasta donde está limitada.

CAPÍTULO 2.MARCO TEÓRICO: En este capítulo se explican los conceptos teóricos básicos que deben ser conocidos para comprender el resto del trabajo realizado en esta Tesis. Primero se habla de los conceptos básicos de una red MPLS -VPN, los protocolos

y tecnologías que las conforman. Luego se describen los diferentes modelos de INTER-AS MPLS-VPNS que serán implementados y sometidos a diferentes pruebas.

CAPÍTULO 3.PARÁMETROS Y HERRAMIENTAS: En este capítulo se describen los programas y aplicaciones utilizadas para la elaboración de esta tesis, tanto de gestión de equipos utilizadas en el entorno de producción, como las que se han utilizado para la elaboración de la memoria.

CAPÍTULO 4.INGENIERÍA DEL PROYECTO: En este capítulo se detallan las pruebas de desempeño de las implementaciones de cada uno de diferentes modelos de INTER-AS MPLS-VPNS, con el objetivo de conocer las ventajas, desventajas, problemas y las posibles soluciones que ofrecen cada una de los modelos. Además se aborda la implementación de la propuesta técnica para la implementación de la red, utilizando el modelo que genera los mejores resultados y que garantiza la escalabilidad y calidad de servicio que las empresas requieren para sus VPNs.

Finalmente, se establece las conclusiones logradas luego de desarrollar esta tesis y se muestran las futuras líneas de trabajo que han surgido por medio del trabajo realizado.

CAPÍTULO 2

MARCO TEÓRICO

2.1 MPLS

2.1.1 Definición (García, 2009)

La conmutación de etiquetas multiprotocolo (MPLS) es una tecnología WAN multiprotocolo de alto rendimiento que trabaja entre las capas 2 y 3 del modelo OSI. Transporta los datos de un router al siguiente según las etiquetas de ruta de acceso corta, en vez de las direcciones de red IP. Para ello, se inserta entre las cabeceras de los protocolos capa 2 y capa 3 la cabecera de 32 bits mostrada en la figura 2.1

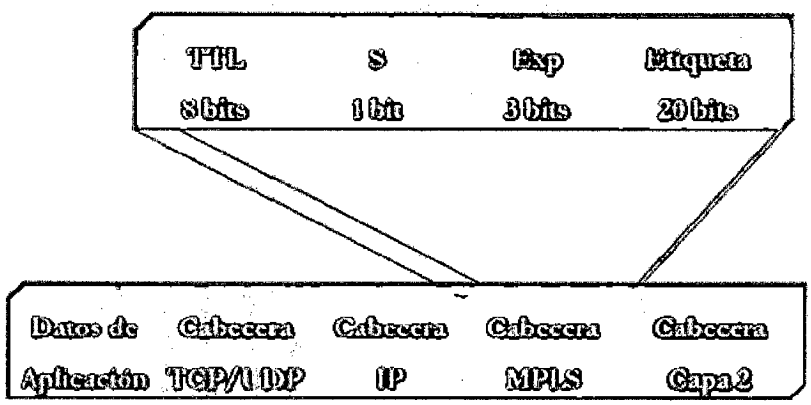


Figura 2.1 Paquete con etiqueta MPLS (García, 2009)

MPLS tiene varias características que la definen. Es multiprotocolo, lo que significa que tiene la capacidad de transportar cualquier contenido, incluido tráfico IPv4, IPv6, Ethernet, ATM, DSL y Frame Relay. Usa etiquetas que le señalan al router qué hacer con un paquete. Las etiquetas identifican las rutas entre routers distantes —en lugar de entre terminales—, y mientras MPLS enruta paquetes IPv4 e IPv6 efectivamente, todo lo demás se conmuta.

MPLS es una tecnología de proveedor de servicios. Las líneas arrendadas entregan bits entre sitios, y Frame Relay y WAN Ethernet entregan tramas entre los sitios. Sin embargo, MPLS puede entregar cualquier tipo de paquete entre sitios. MPLS puede encapsular paquetes de diversos protocolos de red. Admite una amplia variedad de tecnologías WAN, que incluyen los enlaces de portadoras T y E, Carrier Ethernet, ATM, Frame Relay y DSL.

2.1.2 Modos de encapsulamiento MPLS (García, 2009)

MPLS posee dos modos de funcionamiento:

- Modo Trama MPLS: se añade una etiqueta de 32 bits de cuatro campos entre las cabeceras de capa de Red y Enlace.
- Modo Celda MPLS: se utilizan los campos VPI/VCI de la cabecera ATM como etiqueta.

Entre estos dos modos, el más utilizado es el modo Trama el cual será el que se detallará en los siguientes puntos.

2.1.3 Terminología MPLS

Para entender el funcionamiento de MPLS, es importante tener en cuenta los siguientes conceptos previos:

- Forwarding Equivalence Class (FEC): conjunto de paquetes que entran en la red MPLS por la misma interfaz, que reciben la misma etiqueta y por tanto circulan por un mismo trayecto. Normalmente se trata de paquetes que pertenecen a un mismo flujo.
- Label Switched Path (LSP): camino que siguen los paquetes que pertenecen a la misma FEC, es equivalente a un circuito virtual.
- Label Switching Router (LSR): router interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos.
- Edge Label Switch Router (ELSR) o LER (Label Edge Router): router de borde que maneja tráfico entrante y saliente de la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida la extrae y enruta según la capa de Red
- Label Distribution Protocol (LDP): protocolo utilizado para distribución de etiquetas MPLS.
- Tag Distribution Protocol (TDP): Protocolo similar a LDP, propietario de Cisco.
- AS (Sistema Autónomo): un sistema autónomo consiste en un grupo de routers que comparten las mismas políticas de enrutamiento, y están bajo un mismo dominio administrativo.

2.1.4 Modo de funcionamiento (Herrera & Hinojosa, 2009)

Un dominio MPLS está formado por un conjunto de nodos que pueden ser: LERs denominados también routers de acceso y LSRs denominados también routers de tránsito, estos routers son capaces de conmutar y enviar los paquetes en base a la etiqueta añadida a cada paquete.

Las etiquetas determinan un flujo de paquetes entre dos puntos terminales; este flujo se denomina FEC, el mismo que crea un camino particular llamado LSP y contiene los requisitos de calidad de servicio. A continuación se describe el funcionamiento de MPLS, ver figura 2.2.

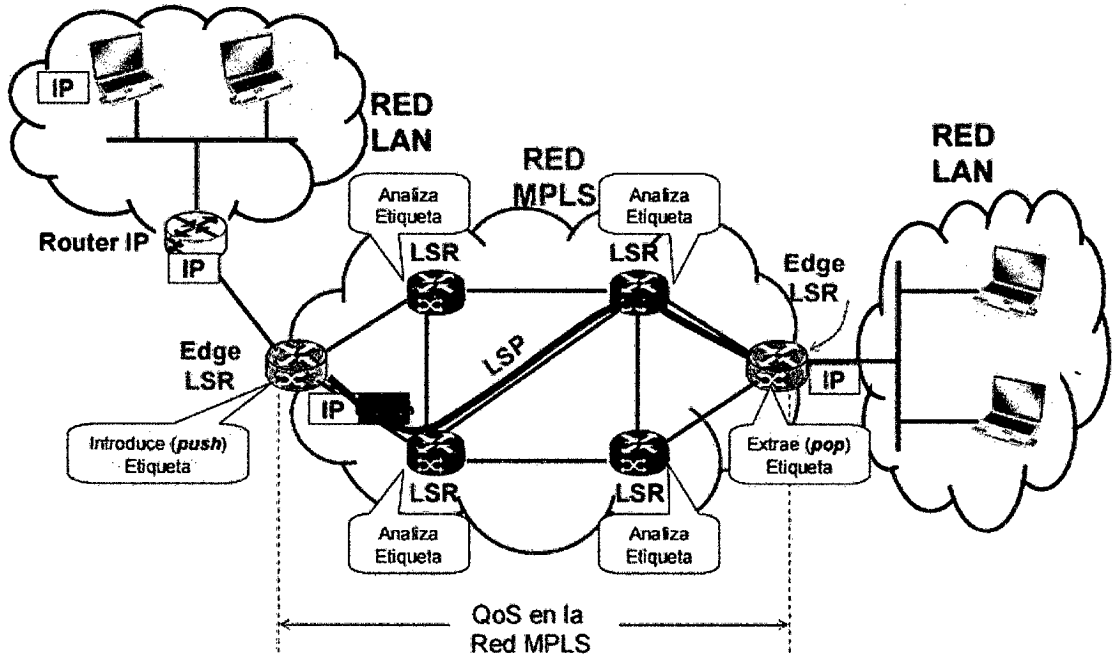


Figura 2.2 Funcionamiento MPLS (Fuente)

Antes de enviar la información se debe determinar un LSP y establecer los parámetros de calidad de servicio para dicho camino. Los parámetros de QoS sirven para comprobar:

- La cantidad de recursos a reservar al LSP.
- Las políticas de descarte de paquetes y prioridades en colas en cada LSR.

Para lograr lo mencionado anteriormente se utilizan dos protocolos para el intercambio de información entre los routers:

- El protocolo OSPF es utilizado para intercambiar información sobre la topología, y el enrutamiento en sí.
- Para determinar los LSPs y establecer las etiquetas entre los siguientes LSRs se puede utilizar el protocolo LDP o el protocolo RSVP-TE (Resource Reservation Protocol Traffic Engineering), también se lo puede realizar manualmente.

Un paquete ingresa al dominio MPLS a través de un router de acceso (LER), este router determina los parámetros de QoS, le asigna un FEC específico al paquete el cual determina un LSP, se etiqueta y se envía el paquete.

Si no existe un LSP para este FEC, el LER junto con los otros routers definen un nuevo LSP. El administrador de red para determinar un FEC debe considerar uno o varios de los siguientes parámetros:

- Direcciones IP de origen o destino y/o direcciones IP de la red.
- Número de puerto de origen o destino.
- Punto de código de servicios diferenciados.
- ID del protocolo IP.
- Flujo de etiquetas IPv6.

El paquete enviado por el LER es recibido por un router de tránsito (LSR), en este momento el paquete se encuentra dentro del dominio MPLS.

El LSR realiza las siguientes funciones:

- Desecha la etiqueta del paquete entrante y añade una nueva etiqueta al paquete saliente.
- Envía el paquete al próximo LSR dentro del LSP.
- El LER de salida desecha la etiqueta, lee la cabecera del paquete IP y envía el paquete a su destino final.

En la figura 2.3 se muestra el funcionamiento del manejo y envío de etiquetas. Cada LSR mantiene una tabla de envío para cada LSP. Cuando un paquete etiquetado llega, el LSR utiliza el valor de la etiqueta como un índice dentro de la tabla de envío LFIB, determina el próximo salto y la nueva etiqueta a ser utilizada, el LSR quita la etiqueta del paquete entrante y añade una nueva etiqueta al paquete saliente.

En la figura 2.3 se observa que al llegar un paquete IP al LER de entrada, éste le añade una etiqueta con valor 8, el siguiente router (LSR) consulta el campo etiqueta de entrada en su tabla buscando el 8, para su interfaz de entrada 4 y cambia el valor de entrada 8 por un 6, así sucesivamente continúa el manejo y envío de etiquetas en una red MPLS.

Pero en el caso de que el tercer router ubicado a la derecha de la figura 2.3 sea el destino, es decir el LER de salida, se debe quitar la etiqueta de entrada y poner el valor del paquete IP enviado.

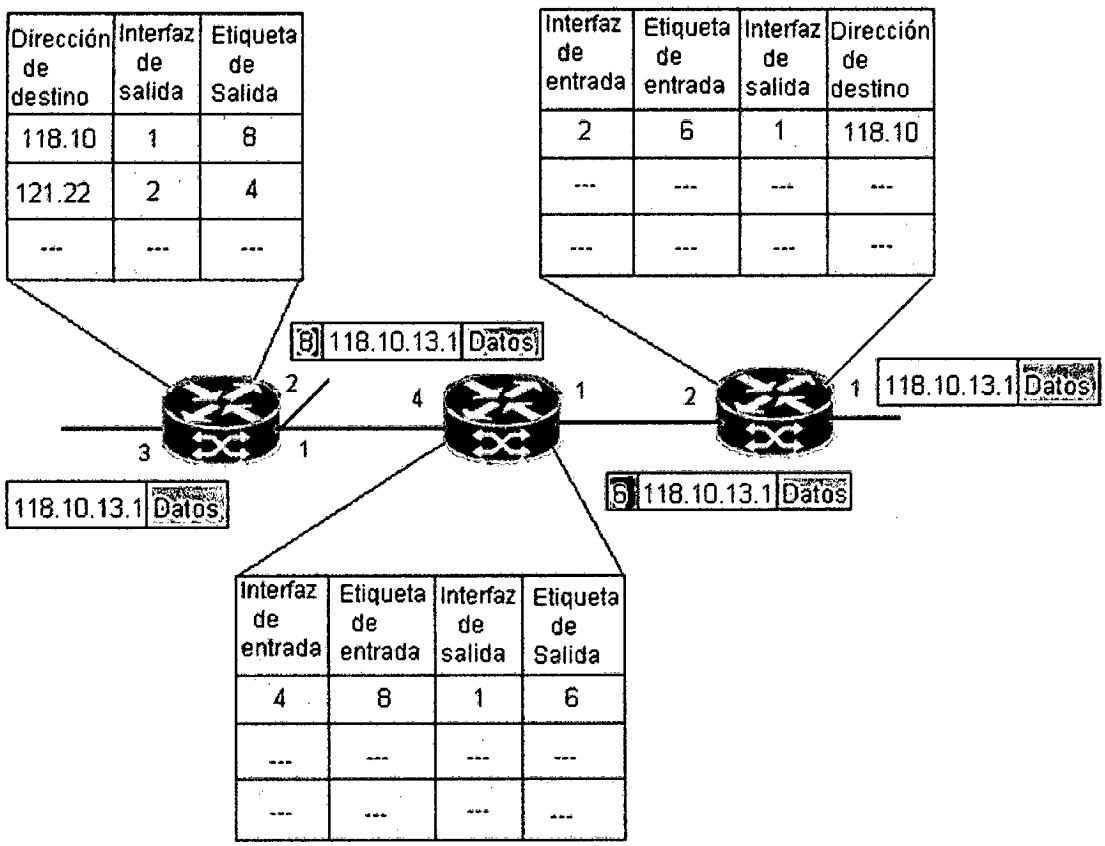


Figura 2.3 Funcionamiento del manejo y envío de etiquetas (Herrera & Hinojosa, 2009)

2.1.5 Arquitectura MPLS (Chica & Samaniego, 2008)

Normalmente MPLS se describe mediante un modelo de arquitectura basado en dos planos:

- Plano de control (control plane): utilizado por los protocolos de routing IP y los protocolos de gestión de MPLS.
- Plano de datos (data plane): en este plano donde se realiza la conmutación de los paquetes.

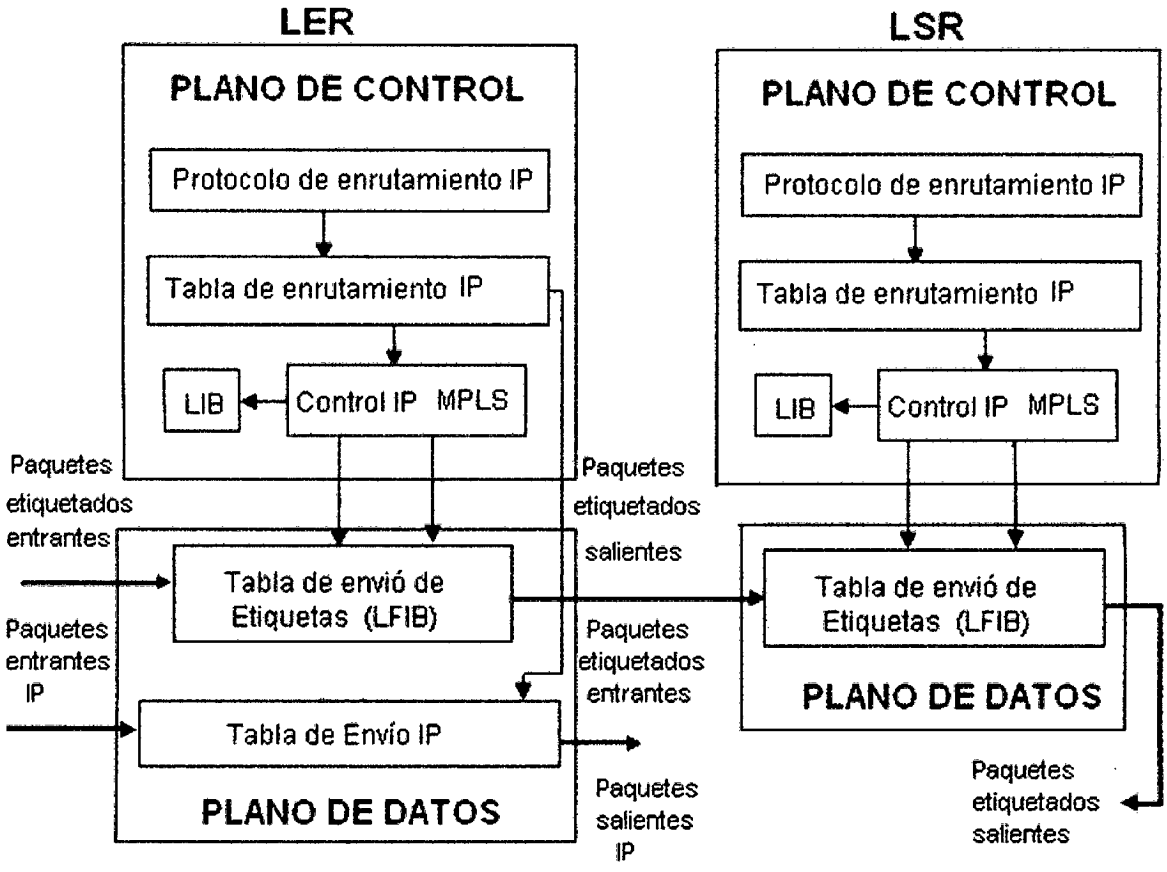


Figura 2.4 Plano de control y de datos (Gonzales Bojorges, 2012)

El **plano de control** se encarga de lidiar con las complejidades del enrutamiento en general éste incluye protocolos como OSPF, EIGRP IS-IS, BGP, etc. Además de los típicos protocolos de enrutamiento existen protocolos de distribución de etiquetas como TDP (Tag Distribution Protocol) y LDP (Label Distribution Protocol). TDP es el predecesor y fue creado por Cisco. Una vez que este protocolo comenzó a dar los resultados esperados solventando los problemas de tráfico con etiquetas, se creó un estándar como el LDP.

El **plano de datos** lleva a cabo tareas relacionadas con el forwarding o envío de paquetes. Estos paquetes pueden ser ya sea paquetes IP o paquetes IP etiquetados. La información en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen del plano de control

Los procesos y funciones de cada plano, originan información que permite publicar o generar tablas que mencionaremos a continuación:

- **RIB (Tabla de Ruteo IP).-** Contiene información originada por el protocolo de enrutamiento (IGP), está situada en el plano de control y muestra información IP–IP.
- **LIB (Base de Información de Etiquetas).-** Esta situada en el plano de control y es originada por el protocolo de distribución de Etiquetas (LDP), contiene información del siguiente salto, como la etiqueta de salida de acuerdo a una dirección IP destino.
- **FIB (Base de Información de Envió).-** Esta situada en el plano de datos, y es una imagen de la tabla RIB, mapea las redes destinos y los ruteadores adyacentes.
- **LFIB (Base de Información de Envió de Etiquetas).-** Está situada en el plano de datos, utiliza información de la tabla FIB y LIB para generar una tabla de etiquetas entrantes y salientes.

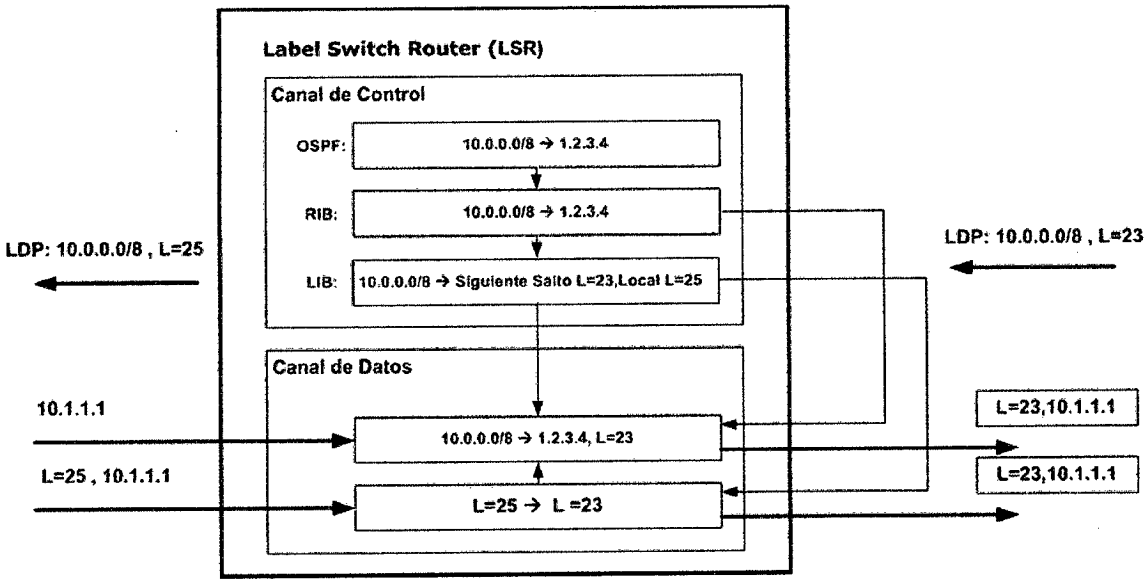


Figura 2.5 Datos del plano de control y plano de datos (Chica & Samaniego, 2008)

2.1.5.1 Etiqueta MPLS (Herrera & Hinojosa, 2009)

MPLS, tal cual ocurre en el enrutamiento tradicional, se basa en los destinos. Las funciones de las etiquetas MPLS son separar las operaciones de envío desde los destinos de capa 3 contenidos en la cabecera de los paquetes asociando una etiqueta con una FEC (Forwarding Equivalence Class). Siendo éste un mecanismo altamente eficiente para el envío de información. La etiqueta MPLS está conformada por 32 bits, divididos en cuatro campos que son los siguientes. Ver figura 2.6.

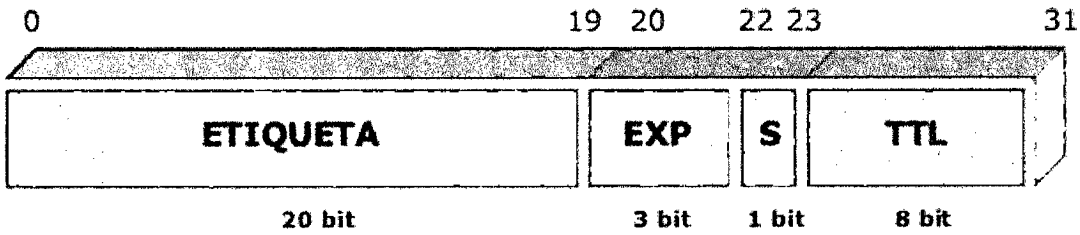


Figura 2.6 Estructura de una etiqueta MPLS (Gonzáles, 2014)

• Etiqueta o Label, campo de 20 bits, este campo contiene el valor de la etiqueta y proporciona la información sobre el protocolo de nivel de red así como información adicional necesaria para reenviar el paquete. La tabla 2.1 contiene los valores de etiquetas reservadas.

Etiqueta	Descripción
0	El paquete proviene de una red IPv4
1	Etiqueta alerta del ruteador
2	El paquete proviene de una red IPv6
3	Etiqueta nula implícita
4 a la 15	Reservados para uso futuro por la Agencia de Asignación de Números de Internet

Tabla 2.1 Etiquetas reservadas en MPLS (Herrera & Hinojosa, 2009)

• Experimental CoS, campo de 3 bits, es el campo reservado para uso experimental, indica la clase de servicio (CoS); el valor de este campo afecta a los algoritmos de planificación y/o descarte que se aplican al paquete a medida que se transmite a través de la red.

• Bottom of Stack Indicator (S), campo de 1 bit, es el campo de posición de la pila. Si tiene el valor de 1 indica que es la última etiqueta añadida al paquete IP, si es un 0 indica que hay más etiquetas añadidas al paquete

• Time To Live (TTL), campo de 8 bits, es un identificador similar a IP, su valor es reducido en cada nodo LSR ,puede ser equivalente al del paquete IP , si su valor es 0 y el paquete aún no alcanza su destino el paquete será descartado.

2.1.5.2 Pila de etiquetas (Chica & Samaniego, 2008)

Una pila de etiquetas es un conjunto ordenado de etiquetas donde cada etiqueta tiene una función específica. La pila de etiquetas es utilizada en varias aplicaciones como: VPNs de Capa3 (L3 MPLS VPN) donde la segunda etiqueta de la pila indica la etiqueta

VPN, Ingeniería de Trafico (MPLS TE) donde el tope de la pila indica el punto final del túnel y la segunda etiqueta identifica el destino y L2 MPLS VPN donde el tope de la pila indica la cabecera del túnel y la segunda etiqueta el Circuito Virtual.

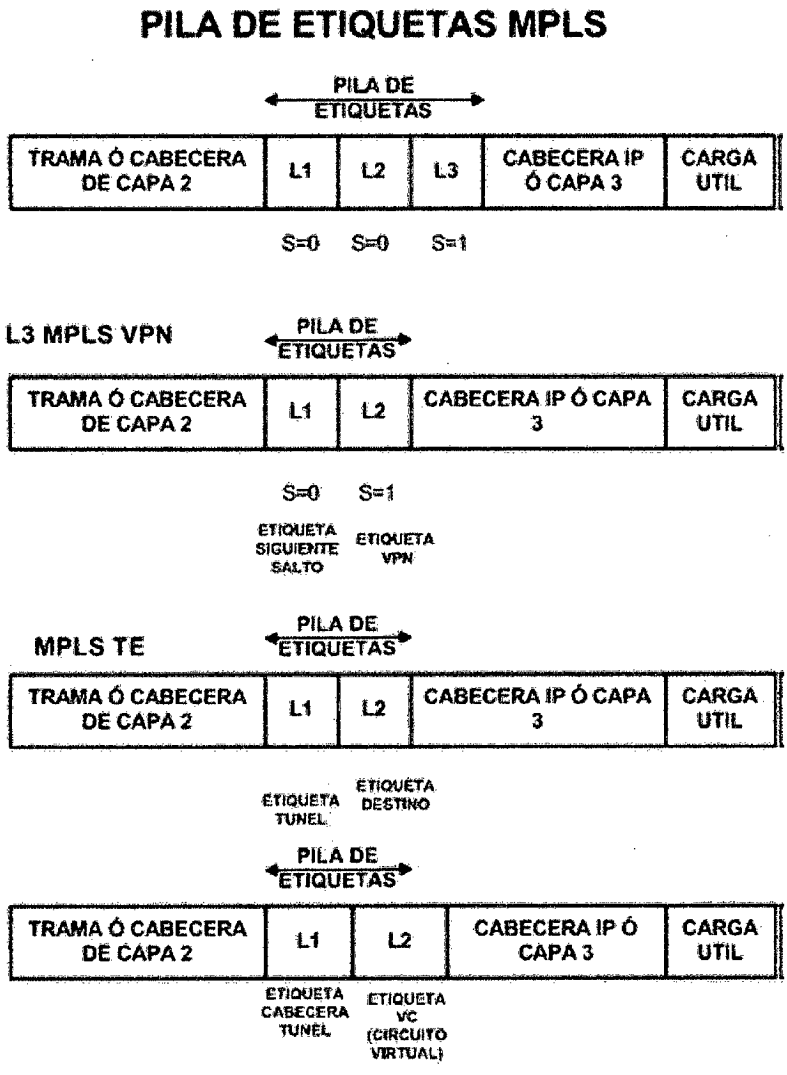


Figura 2.7 Pila de Etiquetas (Chica & Samaniego, 2008)

2.1.5.3 Tipos Especiales de Etiquetas (Chica & Samaniego, 2008)

Existen diferentes tipos de etiquetas dependiendo de su localización en el dominio MPLS de las cuales mencionamos:

Sin etiqueta (Untagged).- Es una etiqueta usada en MPLS VPN para enviar un paquete del dominio MPLS a un dominio de destino diferente.

Etiqueta Nula implícita (Implicit-null).- Esta etiqueta es asignada y distribuida por un LSR, para indicarle al siguiente salto que la etiqueta debe ser removida de la pila,

resultando un paquete sin MPLS. El valor para esta etiqueta es 3 y es usada en las redes MPLS en el Penúltimo Salto o penultimate-hop-popping (PHP).

Etiqueta Nula Explicita (Explicit-null Label).- Es una etiqueta ubicada en el fondo de la pila de etiquetas que nos indica que la operación a realizar es eliminar la etiqueta de la pila y remitir el paquete para que posiblemente sea procesado en base a la cabecera IPv4 o IPv6, su valor puede ser 0 (IPv4) o 2 (Ipv6) . La etiqueta es cambiada con un valor de 0 ó 2 y enviado como un paquete MPLS al próximo-salto. Esta etiqueta es utilizada en la implementación de QoS con MPLS.

Etiqueta de Agregación (Aggregate).- Esta etiqueta permite identificar en una tabla la interfaz de salida cuando un paquete MPLS entrante es convertido a un paquete IP (quitando todas las etiquetas de la pila). Esta etiqueta es usada en las aplicaciones MPLS VPN.

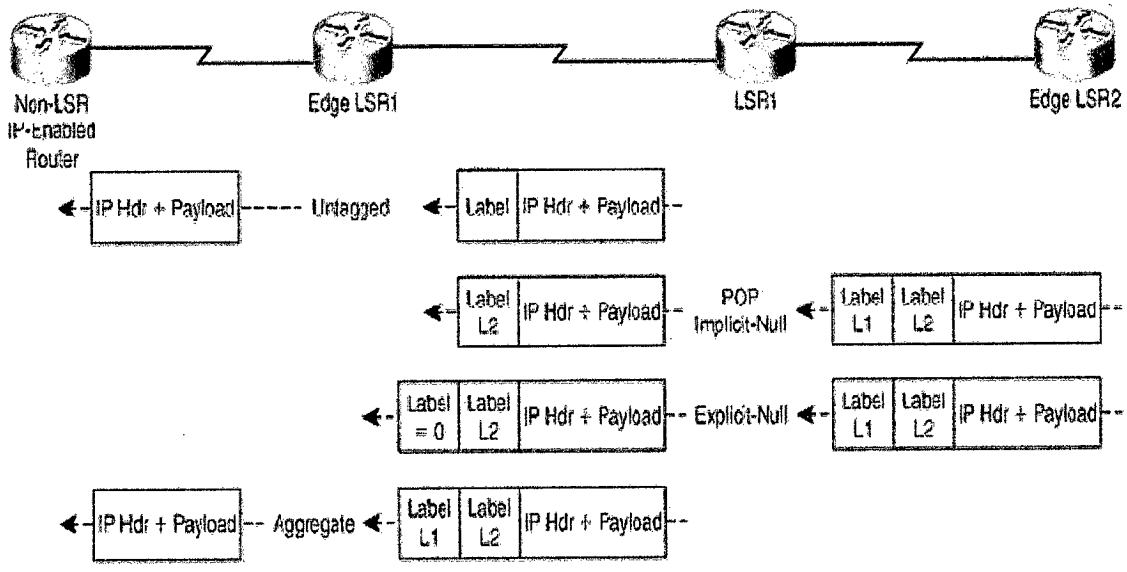


Figura 2.8 Etiquetas especiales de salida (Orozco, 2014)

2.1.5.4 Distribución de etiquetas (González Carrasco, 2011)

La primera etiqueta la pone el LSR de ingreso y pertenece a un LSP. El camino del paquete a través de la red MPLS está definido por el LSP. Todos los cambios se realizan sobre la etiqueta más externa. El LSR de ingreso pone una o más etiquetas, los intermédiate LSR cambian la etiqueta externa, la de entrada, por otra y transmiten el paquete por el enlace de salida que corresponda. El ELSR del LSP quita todas las etiquetas del LSP y reenvía el paquete al CPE que corresponda.

Consideremos el ejemplo de IPv4 sobre MPLS, es el ejemplo más simple y común en una red MPLS. Todos los LSRs hablan un IPv4 Interior Gateway Protocol (IGP) como pueden ser OSPF, ISISI, EIGRP, etc. El LSR de ingreso mira la dirección IP destino del paquete, le pone la etiqueta y reenvía el paquete. El siguiente LSR recibe el paquete etiquetado, cambia la etiqueta más externa por otra y reenvía el paquete por el enlace correspondiente. El ELSR quita todas las etiquetas y envía el paquete IP por el enlace de salida adecuado. Para este proceso, todos los LSRs adyacentes deben estar de acuerdo que etiquetas usar para cada prefijo IGP. Por lo tanto cada intermédiate LSR debe estar capacitado para decidir con que etiqueta de salida debe intercambiar la etiqueta de entrada. Esto significa que es necesario un mecanismo para que los routers sepan que etiquetas usar a la hora de encaminar un paquete. Las etiquetas son locales a cada par de routers adyacentes y no tienen sentido global para cruzar la red. Los routers adyacentes necesitan alguna forma de comunicación entre ellos para estar de acuerdo en que etiqueta usar para cada prefijo; los routers no saben que etiqueta de salida necesitan para sustituir cada etiqueta de entrada por si solos, es necesario un protocolo de distribución de etiquetas.

La distribución de etiquetas se puede hacer de dos formas:

- Distribución de etiquetas junto con la información de routing
- Utilizar un protocolo de routing específico para la distribución de etiquetas

2.1.5.4.1 Distribución de etiquetas junto con la información de routing

Este método tiene la ventaja de que no es necesario otro protocolo distinto para la distribución de etiquetas aunque no es sencillo de implementar y mantener. La gran ventaja de este método es que está sincronizado el intercambio de prefijos y el de etiquetas, por lo que nunca se distribuirá por la red prefijos sin etiquetas ni etiquetas sin prefijos. Esto elimina la necesidad de otro protocolo ejecutándose en el nodo MPLS con las ventajas de consumo de recursos en el router que esto supone. La implementación de un protocolo del tipo vector distancia (como pudiera ser EIGRP) está altamente recomendado ya que cada router origina un prefijo desde su tabla de rutas, entonces el router asocia una etiqueta a cada prefijo que tenga.

Los protocolos del tipo estado de enlace (OSPF e IS-IS) no funcionan de esta manera. Cada router origina actualizaciones de estados de enlace que son reenviados sin

modificar por todos los routers dentro de una misma área. El problema es que para que MPLS funcione, cada router necesita distribuir una etiqueta por cada prefijo que tenga el IGP en su tabla de rutas incluso si los routers no son los que originan este prefijo.

De todos los IGPs ninguno ha evolucionado para desarrollar este método, sin embargo, BGP puede transportar prefijos y etiquetas de manera eficiente. Pero BGP no es un IGP por lo que transporta prefijos externos y se usa principalmente para la distribución de etiquetas en las VPN MPLS.

2.1.5.4.2 Utilizar un protocolo de routing específico para la distribución de etiquetas

Este método tiene la ventaja de que la distribución de rutas se hace en un protocolo dedicado a ello. Independientemente del protocolo de routing que se use y tanto si tiene capacidad de distribución de etiquetas o no, es otro específico el que se encarga de esta tarea. La desventaja de esta opción es que son dos procesos ejecutándose en el nodo.

Para este cometido, el protocolo más usado es LDP, aunque no es el único, ejemplos son TDP, RSVP.

TDP es el precedente de LDP, fue el primer protocolo específico para la distribución de etiquetas, desarrollado e implementado por Cisco. Después el IETF formalizó LDP. LDP y TDP son similares en el modo de funcionamiento pero LDP tiene más funcionalidades de TDP. Incluso en entornos Cisco, LDP fue sustituido por TDP que se ha quedado obsoleto.

2.1.5.5 Distribución de etiquetas con LDP (González Carrasco, 2011)

Para cada prefijo IGP en la tabla de rutas, el nodo crea una asociación local, es decir, asocia cada prefijo con una etiqueta. Entonces el router distribuye esta asociación a todos sus nodos vecinos. Estas asociaciones recibidas se denominan asociaciones remotas. Los vecinos entonces almacenan tanto las asociaciones remotas como las asociaciones locales en una tabla especial, la Label Information Base (LIB). Cada nodo tiene una sola asociación local por cada prefijo, y varias asociaciones remotas ya que lo lógico es tener varios vecinos.

Independientemente de las asociaciones remotas que reciba, el nodo debe seleccionar una sola etiqueta de salida para cada prefijo IP y decidir por enlace reenvía el tráfico. La

tabla de rutas determina cual es el siguiente salto para cada prefijo IP. El nodo elige la asociación remota recibida del siguiente nodo en el camino. Este nodo es el siguiente salto en la tabla de rutas para ese prefijo. Así se va rellenando la Label Forwarding Information Base (LFIB) donde la etiqueta de la asociación local será siempre la etiqueta de entrada y la de salida será la de la asociación remota seleccionada gracias a la tabla de rutas. De esta forma, cuando un nodo recibe un paquete etiquetado, es capaz de intercambiar la etiqueta de entrada por la de salida obtenida del siguiente salto. En la siguiente figura, se muestra como es este intercambio:

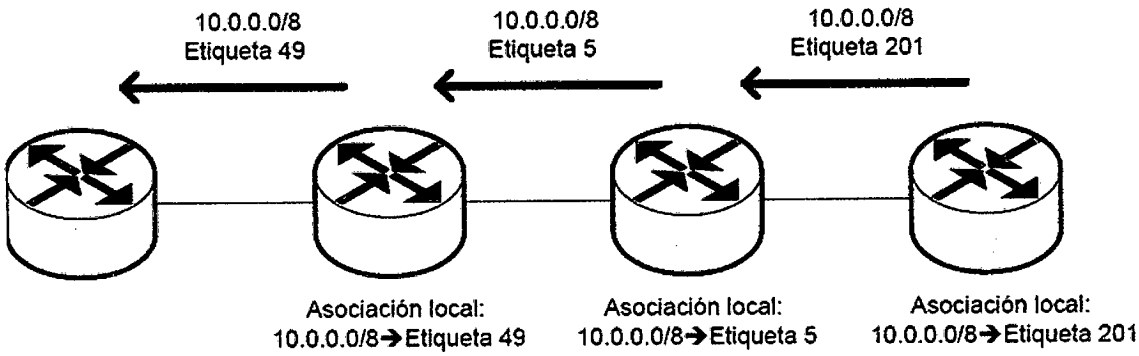


Figura 2.9 Intercambio de etiquetas por LDP para un prefijo (González Carrasco, 2011)

En la siguiente figura se muestra un paquete IP entrando en la red MPLS, se le pone la etiqueta 49 dado el prefijo IP destino y es enviado al siguiente nodo. El segundo nodo, intercambia la etiqueta de entrada (49) por la de salida (5) y envía el paquete hacia el tercer nodo. Este hace lo propio e intercambia la etiqueta de entrada (5) por la de salida (201) y reenvía de nuevo el paquete. Este proceso se repite hasta que sale de la red. Lo vemos gráficamente en la siguiente figura.

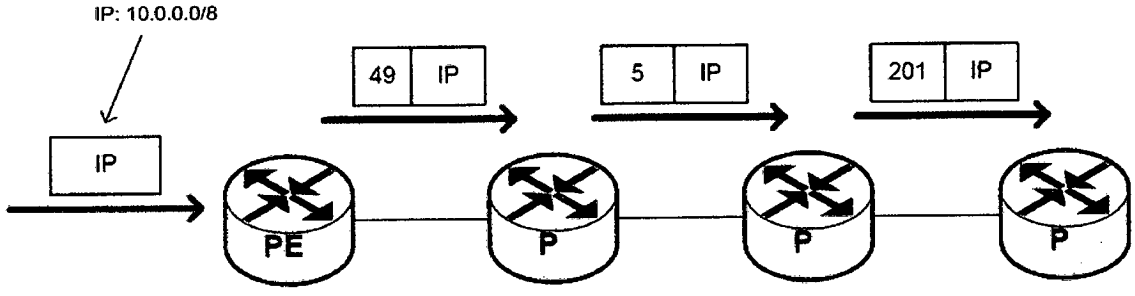


Figura 2.10 Etiquetado de un paquete IP en la red MPLS (González Carrasco, 2011)

2.1.6 Comparación IP y MPLS (Tapasco, 2008)

El surgimiento de MPLS ha sido un gran avance cuando hablamos de eficiencia en la toma de decisiones de enrutamiento y conmutación por parte de un enrutador. En la tecnología IP convencional, cuando un paquete viaja de un lugar a otro, cada enrutador analiza el encabezado capa 3 de cada paquete y se encarga de tomar la decisión de cuál será el próximo salto que el paquete realizará, asignando a éste una FEC, el cual finalmente será enviado a su destino final por medio de un algoritmo de enrutamiento; mientras que con MPLS no es necesario que el paquete sea examinado por cada enrutador debido a que cuando un paquete ingresa al dominio MPLS el primer enrutador conocido como LER asigna una etiqueta al paquete y ésta a su vez asignada a una FEC, entonces como podemos observar estos paquetes son etiquetados antes de ser enviados por el primer LER y como consecuencia de éstos los siguientes enrutadores no tendrán la necesidad de examinar el encabezado de cada uno de los paquetes, sino que utilizarán la etiqueta para relacionarse con una tabla que indica cuál será el próximo enrutador al que el paquete debe ir, este enrutador se encargará de asignar una nueva etiqueta a dicho paquete, sustituyendo la que tenía anteriormente.

Entonces como es de esperarse con MPLS se generan algunas diferencias con respecto a la conmutación tradicional, las cuales son reflejadas en la siguiente tabla:

	Enrutamiento convencional	Conmutación de Etiquetas MPLS
Análisis Encabezado IP.	El análisis del encabezado de los paquetes se realiza en cada uno de los Nodos.	El análisis del encabezado se hace cuando la etiqueta es asignada en el borde de la periferia de la Red.
Soporte de Unicast y Multicast.	Es necesaria la aplicación de diferentes algoritmos complejos para el envío.	Es necesario sólo un algoritmo de envío.
Decisiones de Enrutamiento.	Está basado en direcciones IP.	Se basa en parámetros como QoS.
Base de Datos.	La base de Datos se define con la tabla de enrutamiento IP.	La base de Datos en MPLS se define con la tabla de Clases Equivalentes de Envío FEC.
Protocolos.	Protocolos de enrutamiento IP.	Protocolos de Control que intercambian los contenidos de la tabla FEC entre los LSR.

Tabla 2.2 Comparación entre enrutamiento convencional y conmutación de etiquetas (Tapasco, 2008)

2.1.7 Aplicaciones de MPLS (Reuter & Jiménez, 2013)

Las aplicaciones que ofrece MPLS permiten tener una red eficiente. Las principales facilidades son:

2.1.7.1 Redes Privadas Virtuales (VPN)

Una VPN es una red privada que se puede extender a sitios remotos sobre una infraestructura pública, como Internet. La interconexión a través de la infraestructura pública es transparente para el usuario, aparentando una conexión dentro de un mismo segmento de red por usuarios que en realidad se encuentran en redes distintas. Las VPNs que operan sobre MPLS (VPNs MPLS) se aplican sobre el backbone del proveedor MPLS y garantizan escalabilidad gracias a que se pueden configurar múltiples VPNs para diferentes clientes sin la necesidad de crear cientos de circuitos virtuales.

Las VPNs MPLS permiten que los clientes puedan utilizar cualquier tipo de protocolo de enrutamiento y la dirección IP que deseen (overlapping de direcciones) dentro de su red sin afectar de manera alguna a otros clientes ni al backbone MPLS.

La arquitectura de una VPN MPLS está conformada por dos porciones (ver figura 2.12):

- Red-C: Controlada por el cliente. Aquí se ubica el router CE (Customer Edge).
- Red-P: Controlada por el proveedor. Aquí se ubican los edge LSRs (PE, Provider Edge) y los LSR (P, Provider).

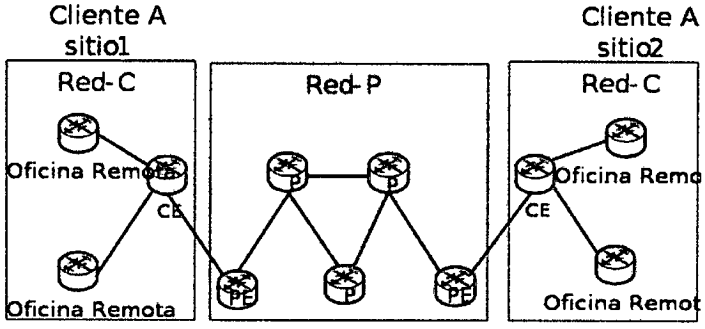


Figura 2.12 Arquitectura de una VPN MPLS (Reuter & Jiménez, 2013)

2.1.7.2 Ingeniería de Tráfico

Mediante la ingeniería de tráfico se puede trasladar parte del tráfico del enlace congestionado (elegido como mejor ruta por el protocolo IGP) a otros menos congestionados o subutilizados, aunque estén fuera de la ruta más corta, ver figura 2.13.

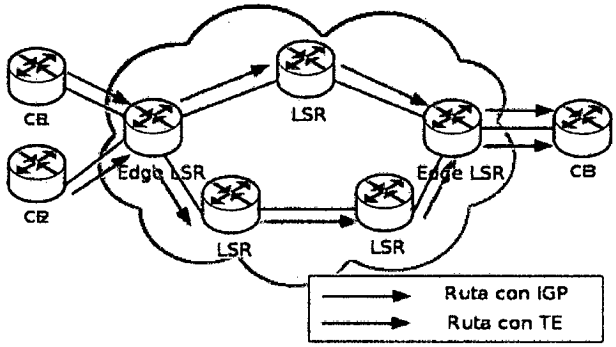


Figura 2.13 Ingeniería de Tráfico vs. mejor ruta del IGP. (Reuter & Jiménez, 2013)

2.1.7.3 Clase de Servicio (CoS)

La Clase de Servicio (CoS) es un término que se usa para diferenciar el tipo de tráfico de una red. Gracias a esta diferenciación se pueden agrupar flujos de paquetes con requisitos semejantes, permitiendo la gestión de diferentes clases de flujos de datos de forma eficaz. La Clase de Servicio (CoS) permite solicitar prioridades para los distintos flujos en base a su importancia.

2.1.7.4 Calidad de Servicio (QoS)

La Calidad de Servicio es el mecanismo que permite que una red pueda asegurar de manera confiable el cumplimiento de requerimientos específicos (retardo, jitter, ancho de banda, pérdida de paquetes y disponibilidad), sin necesidad de sobredimensionar los elementos de la red. La QoS garantiza que las aplicaciones o servicios críticos no se vean afectados por los demás, siendo el cliente quien determina el tipo de tráfico (datos, voz o video) que es crítico para él. En caso de una congestión, el tráfico seleccionado como crítico dispone de mayor prioridad para ser cursado a través de la red.

2.1.8 Ventajas de la tecnología MPLS (Herrera & Hinojosa, 2009)

MPLS brinda las siguientes ventajas:

- MPLS es independiente de la arquitectura de la red y de las redes con las que se interconecta.
- Soporta eficientemente la creación de VPNs.
- Permite el transporte de tráfico con diferente calidad de servicio.
- Permite realizar 'tunneling' de manera más eficiente que IP.
- Soporta escalabilidad de la red, es decir permite expandir la red para incrementar el número de abonados.
- Soporta cualquier tipo de tráfico en una red IP sin depender de los protocolos de enrutamiento, de la capa transporte y de los esquemas de direccionamiento.
- MPLS es una tecnología que permite ofrecer Calidad de Servicio (QoS) independientemente de la red sobre la que se implemente.
- Capacidad para realizar ingeniería de tráfico sin necesidad de que se sobredimensionen los enlaces.
- Soporta tecnologías como ATM, Frame Relay y Ethernet.
- Clasifica con mayor criterio los paquetes en base a FECs y a las interfaces de entrada.

2.2 MPLS con tecnología VPN

Para comprender debidamente la tecnología que ofrecen las VPN sobre MPLS es necesario comprender anticipadamente los posibles problemas que pueden surgir. Las VPN en MPLS son una solución WAN de capa 3 que soluciona el problema de las WAN de capa 2, proporcionando conectividad de muchos a muchos entre sitios de una manera económica y efectiva. En el pasado cada vez que era necesario extender la topología suponía un desembolso importante de dinero lo que siempre hacía difícil dicha extensión. Una topología de malla extendida puede ser muy robusta pero extremadamente costosa, mientras que otras menos caras no ofrecen la solución adecuada. MPLS significó la respuesta y la solución a este problema. Con esta tecnología es posible tener una topología de malla completa pero con la capacidad de hacerlo a nivel de capa 3. La posibilidad de arquitectura que proporciona esta solución es la creación de redes WAN entre los circuitos existentes a nivel de capa 2.

2.2.1 Redes Virtuales Privadas (VPNs)

2.2.1.1 Definición

Una VPN es una red que emula una red privada sobre infraestructura pública existente, como internet. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicio. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas. La figura 2.14 muestra un esquema básico de una VPN.

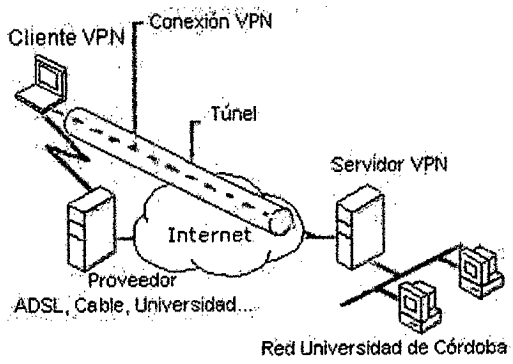


Figura 2.14 Estructura de una red privada virtual (Herrera & Hinojosa, 2009)

2.2.1.2 Beneficios de implementar una VPN

Los beneficios de VPN incluyen lo siguiente:

- Ahorro de costos: las VPN permiten que las organizaciones usen Internet global para conectar oficinas y usuarios remotos al sitio corporativo principal, lo que elimina la necesidad de enlaces WAN dedicados y bancos de módems costosos.
- Seguridad: las VPN proporcionan el nivel máximo de seguridad mediante dos protocolos avanzados de cifrado y autenticación que protegen los datos del acceso no autorizado.
- Escalabilidad: debido a que las VPN usan la infraestructura de Internet en los ISP y los dispositivos, es fácil agregar nuevos usuarios. Las empresas pueden incrementar ampliamente la capacidad, sin agregar una infraestructura significativa.
- Compatibilidad con la tecnología de banda ancha: los proveedores de servicios de banda ancha, como DSL y cable, admiten la tecnología VPN, de modo que los trabajadores móviles y los empleados a distancia pueden aprovechar el servicio de Internet de alta velocidad de sus hogares para acceder a las redes corporativas. Las conexiones de banda ancha de alta velocidad para uso empresarial también pueden proporcionar una solución rentable para la conexión de oficinas remotas.
- Mayor Productividad: las VPN dan un nivel de acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la RED. Además, con la consecutiva reducción en las necesidades de espacio físico, se fomenta el teletrabajo.

2.2.1.3 Modelos de implementación de una VPN (Herrera & Hinojosa, 2009)

Si el router CE del cliente y el proveedor de servicio intercambian información de enrutamiento de capa 3, las VPNs se pueden clasificar en: Modelo Overlay y Modelo Peer to Peer:

2.2.1.3.1 Modelo Overlay VPN o tradicionales

La VPN Overlay es aquella donde el proveedor de servicio y el cliente no intercambian información de enrutamiento de capa 3. En la figura 2.15, este modelo puede implementarse con varias arquitecturas como: X.25, Frame Relay, ATM, etc.

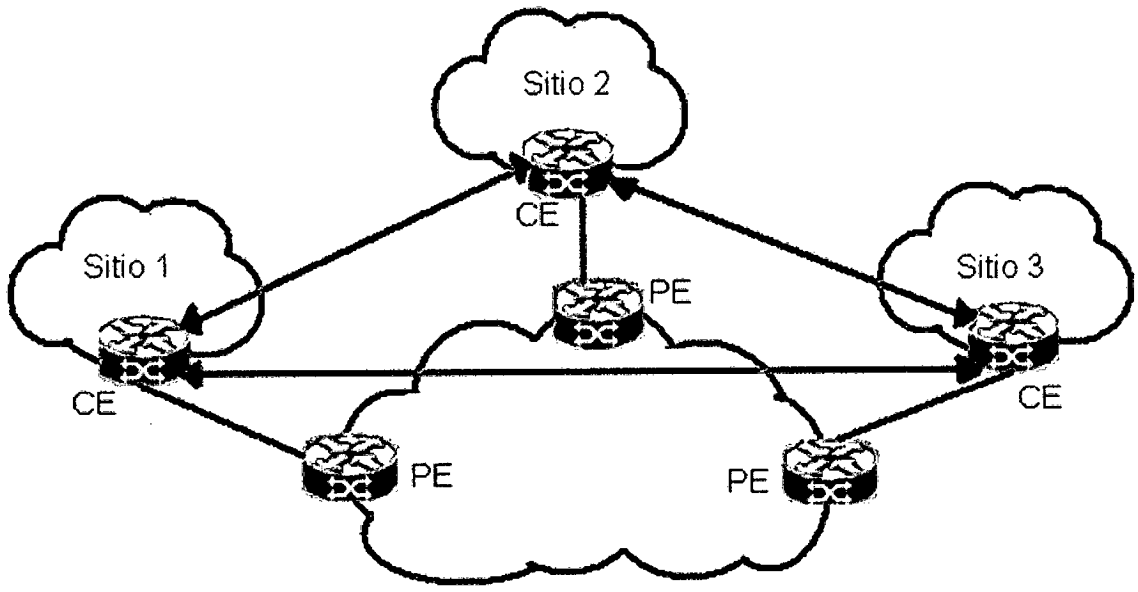


Figura 2.15 Modelo Overlay (Herrera & Hinojosa, 2009)

2.2.1.3.2 Modelo Peer to peer VPN

En el modelo VPN peer-to-peer se intercambia información de enrutamiento entre la VPN y la WAN. Este modelo se introdujo para contrarestar los inconvenientes del modelo Overlay VPN. En el modelo peer-to-peer, el equipo de borde del proveedor (PE) es un router que intercambia directamente las rutas con el router CPE. La figura 2.16 muestra un ejemplo de VPN peer-to-peer.

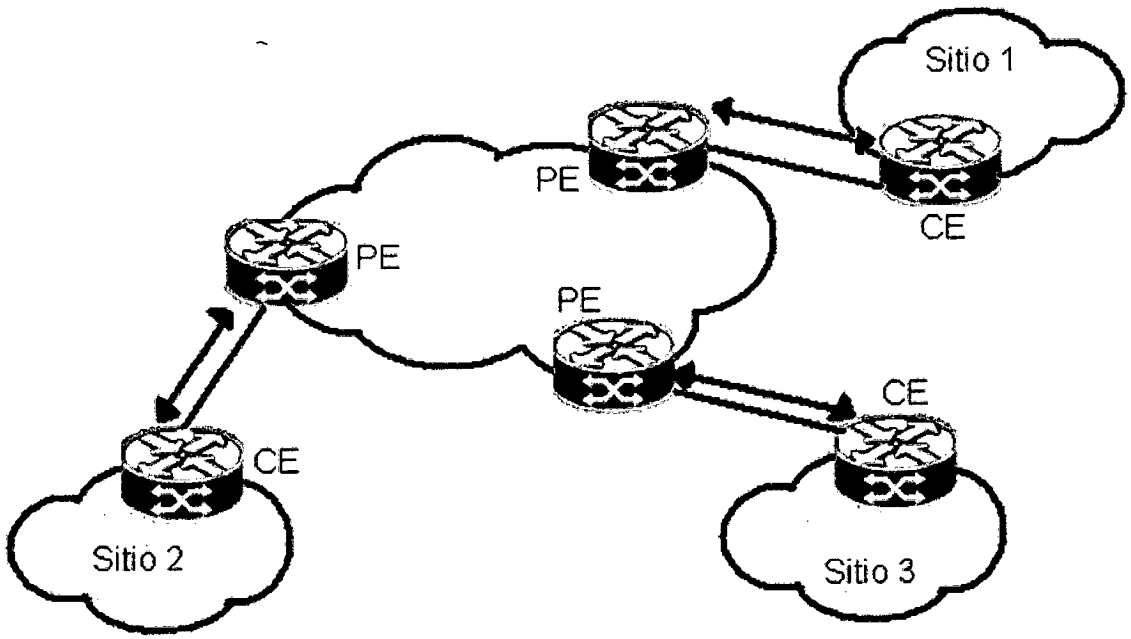


Figura 2.16 Modelo peer-to-peer (Herrera & Hinojosa, 2009)

2.2.2 MPLS VPN

Las MPLS VPNs o redes privadas virtuales MPLS, es la más popular y usada implementación de la tecnología MPLS. Una red privada requiere que todos los locales del cliente puedan interconectarse y sean completamente separadas de otras VPNs. Ese es el mínimo requisito de interconectividad que debe cumplirse. Sin embargo, algunos modelos de VPN de Capa 3 pueden requerir más que eso. Deben ser capaces de brindar conectividad entre diferentes VPNs e incluso proveer conexión a Internet. Las MPLS-VPNs ofrecen todo lo anterior, lo cual es posible debido a que existe un desacoplamiento del plano de datos y el plano de control que no es posible con IP.

2.2.2.1 Terminología de MPLS VPN

Muchas de las terminologías de MPLS VPN han sido explicadas anteriormente, sin embargo el resumen y otros términos agregados son los siguientes:

- Red C: red interna del cliente.
- Red P: red del proveedor de servicio.
- Router CE: es el router del cliente que se conecta al PE.
- Router PE: es el router MPLS del ISP que se conecta al router CE. Maneja e intercambia la información de las VPNs utilizando una extensión del protocolo BGP llamada Multiprotocol BGP (MP-BGP).
- Router P: es el router MPLS en el core o backbone de la red y nunca está de cara al cliente. No tiene conocimientos de las VPNs, tan solo se encargan del transporte para los paquetes que los PE intercambian.
- Router RR: es el router utilizado para distribuir tablas de enrutamiento y disminuir el número de conexiones.
- Label-Switched Path (LSP): es la ruta establecida para el uso de etiquetas en los paquetes a través de la red P en el tránsito hacia un destino en particular.
- Penultimate Hop Pop (PHP): es el router P anterior al router P de destino y que se encarga de quitar la etiqueta y entregar el paquete al router PE.
- VRF (VPN Routing & Forwarding instance): es una tecnología que permite la coexistencia de varias tablas de enrutamiento dentro del mismo router al mismo tiempo. Pueden existir múltiples VRFs en los PE para aislar las tablas de enrutamiento de distintos clientes.
- RD (Route Distinguisher): Es un identificador de 64 bits que se antepone a la dirección de red para formar un prefijo único. En el caso de IPv4 (32 bits) se forma un prefijo llamado VPNv4 de 96 bits

- RT (Route Target): Asocia las VRF a VPNs. Con este atributo, una VRF puede pertenecer a una o varias VPNs, pudiendo crear esquemas complejos de VPNs.
- MP-BGP (Multiprotocol BGP): Es una extensión del protocolo BGP que sirve para propagar direcciones como VPNv4 y los atributos que las acompañan (p.e. RT). El protocolo es utilizado solamente entre PEs.

2.2.2.2 Modelo MPLS VPN (González Carrasco, 2011)

En la siguiente figura se muestra un esquema general del modelo MPLS VPN:

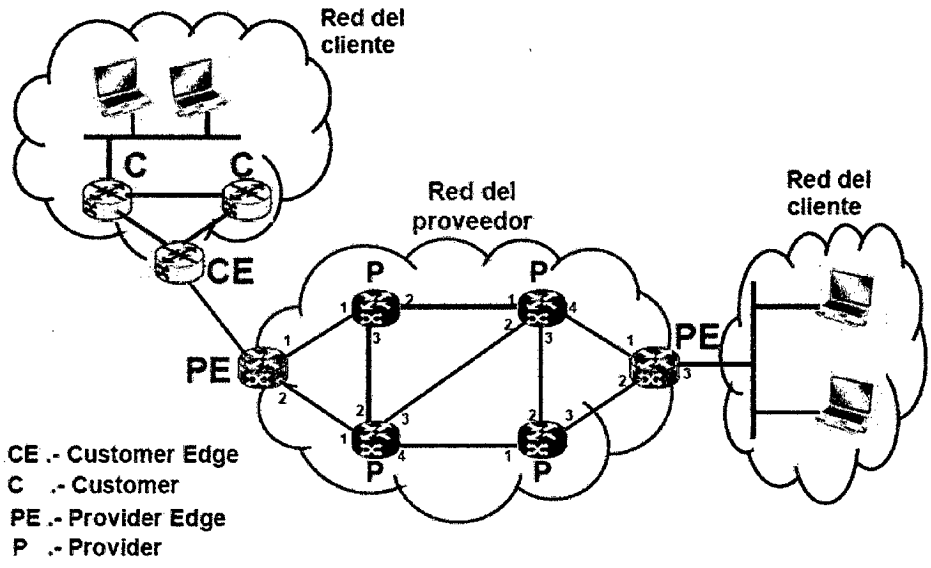


Figura 2.17 Esquema general MPLS VPN (González Carrasco, 2011)

Debido a que tanto los routers CE como los PE interactúan a nivel 3, es necesario que trabajen con un protocolo de enrutamiento dinámico (o rutas estáticas). El CE solo tiene un equipo conectado fuera de su ubicación, el PE. El CE no tiene conectividad física directa con ningún otro CE. El nombre de este modelo se llama peer-to-peer ya que el CE y el PE tienen una conexión de nivel 3.

Una VPN debe ser privada, por ello los clientes pueden tener su propio plan de direccionamiento, puede usar, tanto direccionamiento público como privado e incluso se puede repetir direccionamiento entre clientes. Si los paquetes fuesen reenviados como paquetes IP en los nodos P habría un problema de enrutamiento. Si no se les permitiese a los clientes tener su propio direccionamiento, este debería ser asignado por el proveedor de servicios. Suponiendo esto, los paquetes podrían ser reenviados atendiendo a su dirección IP destino en cada router de la red del proveedor. Esto significa que tanto los nodos P como los nodos PE deberían tener una tabla de rutas completa con el direccionamiento de cada cliente y esa tabla podría ser muy grande. El

único protocolo de routing capaz de manejar semejante tabla es BGP por lo que tanto nodos P como nodos PE deberían hablar iBGP entre ellos. Llegados a este caso no sería un esquema válido debido a que no es un entorno privado para cada cliente.

Otra solución sería que tanto LSRs P como LSRs PE manejasen tablas de rutas distintas para cada cliente. Debería haber tantos procesos de enrutamiento como VPNs de cliente hubiera configuradas en la red. Esta no es una solución muy escalable ya que cada vez que un nuevo cliente se diese de alta en la red habría que configurar en cada nodo (tanto P, como PE) un proceso de enrutamiento. Además, al entrar un paquete a la red a través de un PE, ¿Cómo se podría identificar a que VPN pertenece? La solución pasaría por modificar el paquete IP añadiéndole un campo de identificación de VPN. Entonces los nodos P deberían mirar además del campo IP destino el campo de VPN para reenviar adecuadamente el paquete. Una solución escalable es que los routers P no tuviesen consciencia de VPN lo que les liberaría de la carga de tener información de las rutas para cada VPN. Precisamente esto es la solución que ofrece MPLS. Los paquetes IP de cada cliente son etiquetados en la red MPLS para conseguir una VPN privada para cada cliente. Además, los routers P no necesitan conocer la tabla de rutas gracias a la utilización de dos etiquetas MPLS. Por lo tanto, BGP no es necesario en los routers P. Las rutas para cada VPN solo se manejan en los routers PE al igual que solo hay concepto de VPN en los PEs lo que hace que las MPLS VPNs sean una solución escalable, tal cual se muestra en la figura 2.18

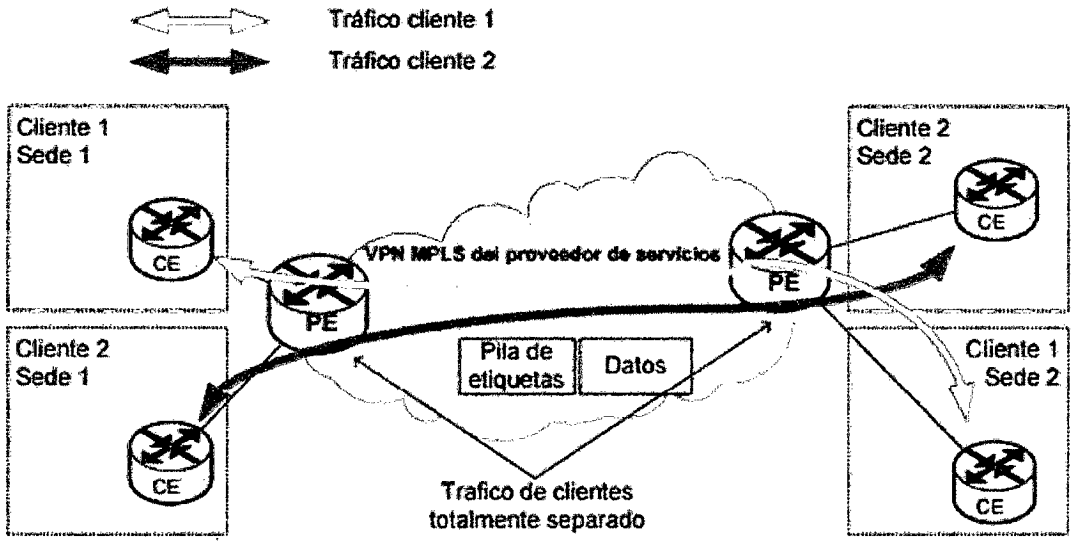


Figura 2.18 Modelo de MPLS VPN (González Carrasco, 2011)

2.2.2.3 Funcionamiento de MPLS-VPN (Gómez & Moliner, 2005)

Con el objetivo de entender el funcionamiento de una red MPLS VPN se presentará un ejemplo hipotético. Imaginemos una empresa proveedora de servicios que ofrece servicios MPLS/VPN. El proveedor de servicio tiene dos puntos de presencia POP (*Point of Presence*), uno que llamaremos PE1 y uno que llamaremos PE2, estando los POPs enlazados a través de dos routers de núcleo nombrados P1 y P2.

En el ejemplo el proveedor tiene dos clientes: Empresa A que conformara la VPN-A, con el sitio-1 y el Sitio-2 conectado a PE1 y el sitio-3 conectado a PE2 y la Empresa B que conformara la VPN-B con el sitio-1 conectado a PE2 y el sitio-2 conectado a PE1. La topología de red es mostrada en la figura 2.19.

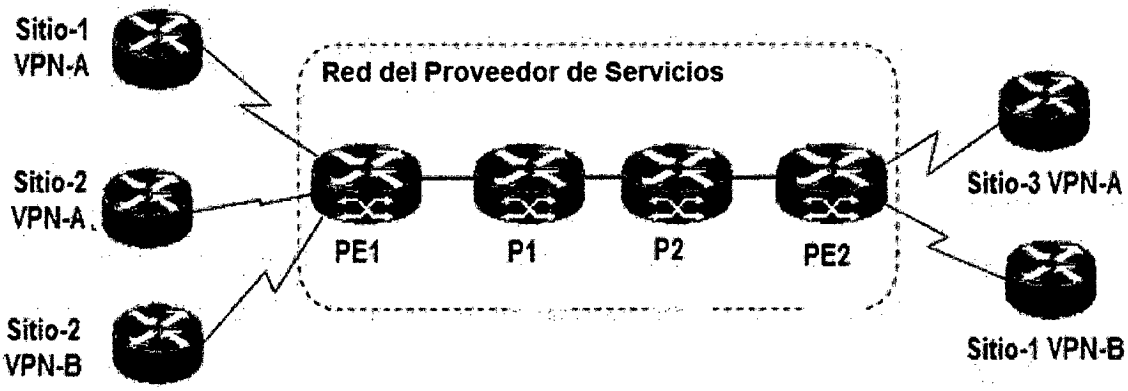


Figura 2.19 Red y sus clientes (Goméz & Moliner, 2005)

Acorde a las siguientes terminologías los routers en la figura 2.19 tienen las siguientes funciones:

- Los routers PE1 y PE2 que enlazan la red con sus clientes son routers de la frontera del proveedor de servicio (PE, Provider Edge).
- Los routers P1 y P2 que no tiene conexiones directas con los clientes son routers del núcleo de la red del proveedor (P, Provider).
- Los routers de los clientes conectados al PE1 en el sitio-1 y sitio-2 de la Empresa A y en el sitio-2 de la Empresa B al igual que los conectados al PE2 en los sitio-1 y sitio-3 de la Empresa B y la Empresa A respectivamente son routers de la frontera del cliente (CE, Customer Edge).

Asumiendo que ambas Empresas la A y B, siguen la misma convención para el direccionamiento de sus VPN, los sitios-1 usan direcciones IP públicas, mientras que los sitios-2 y el sitio-3 de ambas Empresas, usan espacios de direcciones IP privadas (red 10.0.0.0).

El direccionamiento IP usado por estas dos empresas está resumido en la tabla 2.3.

Compañía	Sitio	Subred
Empresa A	Sitio-1	192.168.2.0/24
	Sitio-2	10.5.1.0/24
	Sitio-3	10.5.2.0/24
Empresa B	Sitio-1	192.168.8.0/24
	Sitio-2	10.5.1.0/24

Tabla 2.3 Direccionamiento IP de Empresa A y Empresa B. (Gómez & Moliner, 2005)

El proveedor de servicio pretende ofertar un servicio basado en el modelo peer to peer (no un número de túneles IP sobre IP), pero hay que tener en cuente un número de detalles porque el espacio de direcciones IP de los sitios-2 conectados al mismo router PE1 se solapan. El solapamiento de direcciones usualmente resultado del uso de direcciones IP privadas en las redes de los clientes es uno de los mayores obstáculos para el desarrollo de implementaciones VPN peer to peer. La tecnología MPLS/VPN brinda una solución eficiente a este dilema. Cada VPN tiene su propia tabla de envío y enrutamiento en el router, así cualquier cliente o sitio que pertenezca a una VPN le está sólo permitido el acceso a un grupo de rutas contenidas dentro de la tabla. Cualquier routers PE en una red MPLS/VPN contiene un número de tablas de enrutamiento por VPN y una tabla de enrutamiento global que es usada para alcanzar los otros routers en la red del proveedor, así como destinos alcanzables externos, como por ejemplo, el resto de Internet. Efectivamente un número de routers virtuales son creados en un único router físico, como se muestra en la figura 2.20 para el caso del router PE1 de la red.

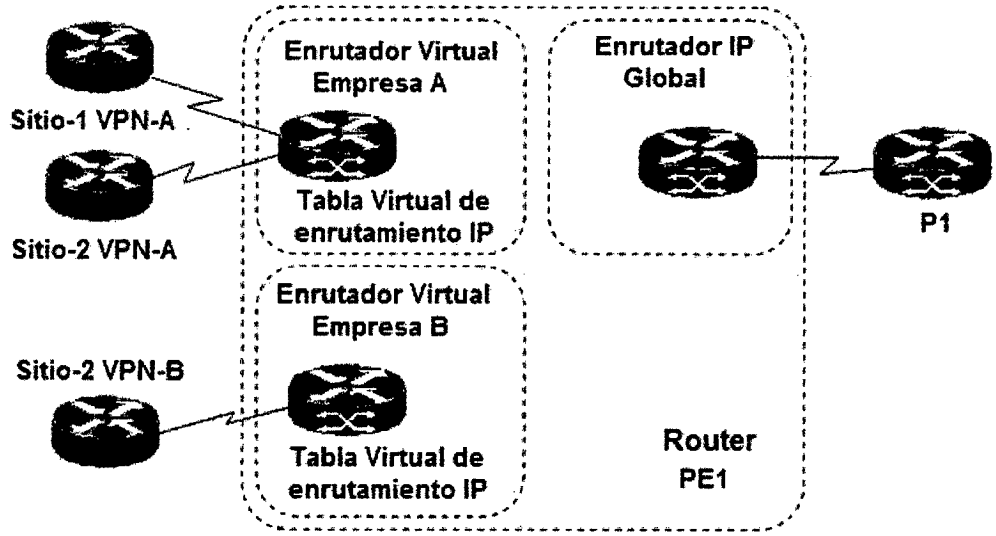


Figura 2.20 Enrutadores Virtuales creados en un enrutador PE1. (Gómez & Moliner, 2005)

El concepto de routers virtuales les permite a los clientes usar cualquier espacio de direcciones globales o privadas en cada VPN. Para cada cliente o sitio perteneciente a una VPN existe un solo requerimiento, que el espacio de direcciones sea único dentro de la VPN. La exclusividad de direcciones no es requerida entre VPNs, excepto cuando dos VPN, que comparten el mismo espacio de direcciones privadas quieran comunicarse.

A cada router virtual no solamente está asociada la tabla de enrutamiento virtual, hay más estructuras comprendidas en el router virtual:

- Una tabla de envío que se obtiene de la tabla de enrutamiento.
- Un grupo de interfaces a usar por la tabla de envío.
- Reglas que controlan la importación y exportación de rutas desde y hacia la tabla de enrutamiento de la VPN.
- Un grupo de protocolos de enrutamiento, los cuales adicionan información en la tabla de enrutamiento de la VPN, incluyendo rutas estáticas.
- Routers asociados con los protocolos de enrutamiento que son usados para llenar la tabla de enrutamiento de la VPN.

La combinación de las tablas de enrutamiento IP VPN y la asociada tabla de envío IP VPN es llamada Instancia de Enrutamiento y Envío VPN (VRF, VPN Routing and Forwarding).

2.2.2.3.1 Interconexión de Redes Privadas Virtuales

El ejemplo del SP utilizado hace creer que una VPN está asociada solamente con un VFR en un enrutador PE, aunque esto puede ser verdad en el caso de que los clientes de las VPN no necesiten conectividad con otras VPN, la situación pude hacerse más compleja y requerir más de un VFR por cliente VPN conectado a un enrutador PE.

Imaginemos que se desea ampliar los servicios ofertados con un servicio de voz sobre IP (VoIP, Voice over IP) con centrales (gateways) a la Red Pública de Voz localizadas en PE1 y PE2, como se muestra en la Figura 2.21.

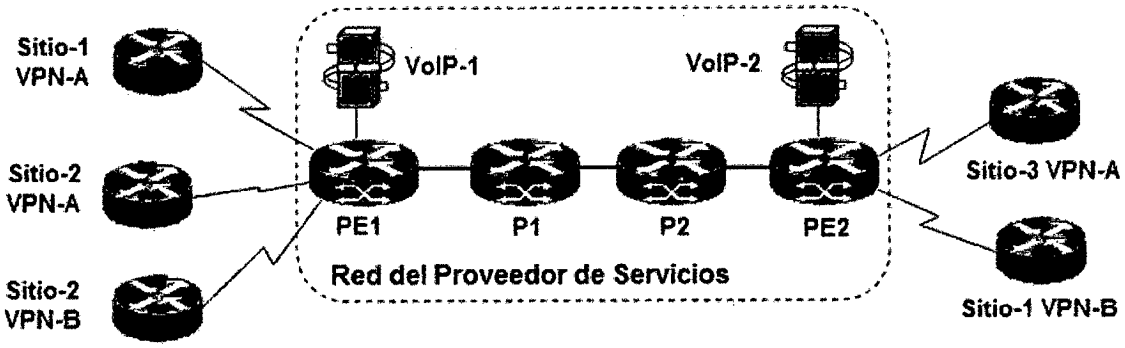


Figura 2.21 Centrales VoIP en la red del proveedor. (Gómez & Moliner, 2005)

Una de las alternativas posibles es situar las centrales de VoIP en una VPN separada que llamaremos VPN-VoIP para incrementar la seguridad del nuevo servicio creado. El direccionamiento IP de las centrales es como se muestra en la tabla 2.4.

Ubicación de la Central VoIP	Dirección IP de la Pasarela VoIP
VoIP-1	200.55.33.32
VoIP-2	200.55.37.15

Tabla 2.4 Direcciones IP de las Centrales VoIP en la red. (Gómez & Moliner, 2005)

Ambos clientes Empresa A y Empresa B deciden usar el servicio de VoIP, pero sólo para sus sitios-1, los demás sitios en el ejemplo no necesitan hacer llamadas de larga distancia. Estos requerimientos nos llevan a un problema interesante, los sitios-1 de ambas compañías necesitan estar en dos VPNs, la VPN de sus empresas para alcanzar sus sitios remotos y la VPN-VoIP para alcanzar las pasarelas de VoIP. La conectividad necesaria se ilustra en la figura 2.22

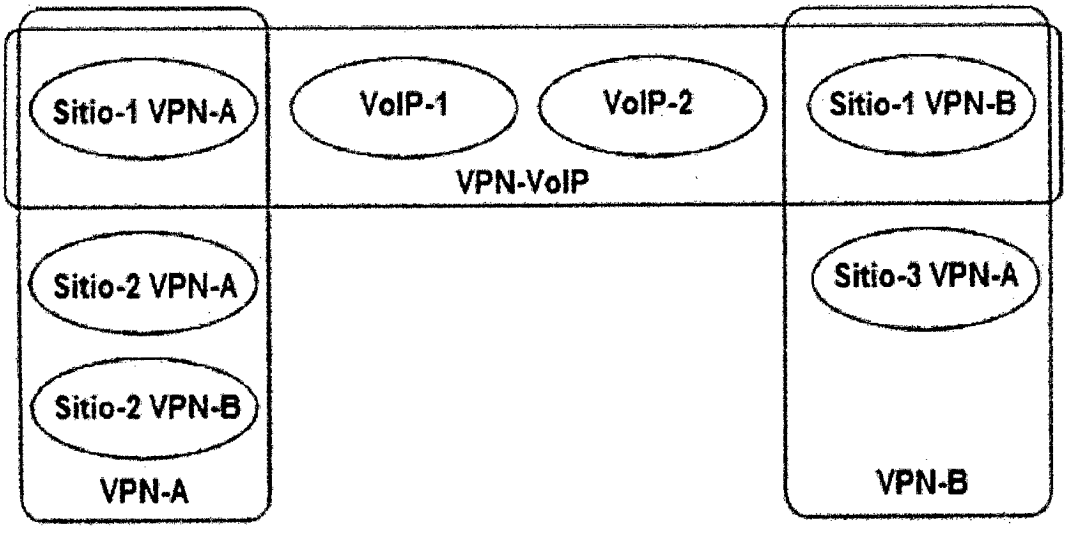


Figura 2.22 Conectividad VPNs en la red del proveedor. (Gómez & Moliner, 2005)

Para soportar requerimientos de conectividad similares a los de la figura 2.22, la arquitectura MPLS/VPN de Capa 3 se apoya en el concepto de sitios (sites), donde una VPN es un arreglo de uno o múltiples sitios. Una VPN es esencialmente una colección de sitios compartiendo información de enrutamiento común, lo cual significa que un sitio puede pertenecer a más de una VPN si este sostiene rutas desde VPN separadas. Esto nos permite construir intranets y extranets, así como cualquier otra topología de las descritas anteriormente. Una VPN en la arquitectura MPLS/VPN puede consecuentemente ser dibujada como una comunidad de intereses o un grupo cerrado de usuarios, lo cual es dictado por la visibilidad de enrutamiento que los sitios puedan tener.

El concepto de VRF introducido anteriormente puede ser modificado para soportar el concepto de sitios que pueden residir en más de una VPN, por ejemplo, el sitio-1 de la Empresa A no pueden usar el mismo VRF que el sitio-2 de la Empresa A conectado al mismo enrutador PE1. El sitio-1 Empresa B necesita acceso a las centrales de VoIP, por lo que las rutas hacia esta central deben estar en el VRF para este sitio. Por lo que VFR es una colección de rutas que pueden estar disponibles para un sitio en particular o para un grupo de sitios conectados a un enrutador PE. Estas rutas pueden pertenecer a más de una VPN. La tabla 2.5 muestra el conjunto de VRFs para la red del proveedor.

Enrutador PE	VRF	Sitios en la VRF	VPNs que pertenecen al VRF
PE1	Sitio-1 Empresa A	Sitio-1 Empresa A	VPN-A, VPN-VoIP
	Sitio-2 Empresa A	Sitio-2 Empresa A	VPN-A
	Sitio-2 Empresa B	Sitio-2 Empresa B	VPN-B
	VoIP-1	Pasarela VoIP-1	VPN-VoIP
PE 2	Sitio-3 Empresa A	Sitio-3 Empresa A	VPN-A
	Sitio-1 Empresa B	Sitio-1 Empresa B	VPN-B, VPN-VoIP
	VoIP-2	Pasarela VoIP-2	VPN-VoIP

Tabla 2.5 VRF en los enrutadores PE de la red. (Gómez & Moliner, 2005)

Con lo estudiado anteriormente se arriba a que no existe un mapeo directo entre una VPN y un VRF, por lo que el enrutador necesita conocer cuales rutas debe insertar en cada VRF. Esto es resuelto con la introducción de otro concepto en la arquitectura MPLS/VPN de Capa 3 las RT (route target), atributo que le permite a un enrutador conocer cuáles rutas insertar en cada VRF. Cuando una ruta VPN es exportada desde un VRF para ser ofertada a otros VRF, esta es etiquetada con una o más RT. También podemos asociar un grupo de RT con un VRF, y todas las rutas etiquetadas con al

menos una de estas RT deben ser insertadas en el VRF. Las RT están conformadas por 64 bits, por motivos de simplificación, se asumen nombres para las RT en esta parte del trabajo.

La red contiene tres VPNs por lo que requiere tres RT, la asociación entre VRFs y RT en la red se observa en la tabla 2.6.

Enrutador PE	VRF	Sitios en el VRF	*Route target* adjuntadas para exportar rutas	*Route target* importadas
PE1	Sitio-1 Empresa A	Sitio-1 Empresa A	Empresa A, VoIP	Empresa A, VoIP
	Sitio-2 Empresa A	Sitio-2 Empresa A	Empresa A	Empresa A
	Sitio-2 Empresa B	Sitio-2 Empresa B	Empresa B	Empresa B
	VoIP-1	Pasarela VoIP-1	VoIP	VoIP
PE2	Empresa A	Sitio-3 Empresa A	Empresa A	Empresa A
	Empresa B	Sitio-1 Empresa B	Empresa B, VoIP	Empresa B, VoIP
	VoIP-2	Pasarela VoIP-2	VoIP	VoIP

Tabla 2.6 Correspondencia entre VRFs y Route targets en red. (Gómez & Moliner, 2005)

2.2.2.3.2 Propagación de información de enrutamiento en la red del proveedor.

Dos vías diferentes existen para el intercambio de información de enrutamiento VPN entre los enrutadores de frontera (PE) del proveedor de servicio.

- Corriendo algoritmos de enrutamiento diferentes en los enrutadores PE para cada VPN, por ejemplo copias de OSPF podrían estar corriendo para cada VPN, solución esta con serios problemas de escalabilidad en SP con gran número de VPN en sus redes.
- Correr un único protocolo de enrutamiento en el enrutador PE para el intercambio de todas las rutas de las VPNs. Con este método para poder soportar el solapamiento de los espacios de direcciones de las VPN, las direcciones IP usadas por los clientes deben ser aumentadas con información adicional que las haga únicas.

Para desarrollar la tecnología MPLS/VPN ha sido seleccionada la segunda de estas estrategias, las subredes IP propagadas por los enrutadores frontera del cliente (CE) serán aumentadas con un prefijo de 64 bits llamado un RD (route distinguisher), atributo que se le adiciona a las direcciones IP para hacerlas únicas en un dominio MPLS. El direccionamiento en las VPN-IPv4 (VPNv4) es la combinación de una

dirección IPv4 y el route distinguisher (Rosen y Rekhteri, 1999). El direccionamiento resultado compuesto por 96 bits será intercambiado entre los PE utilizando un direccionamiento especial de la familia de Multiprotocolos BGP (MP-BGP). Existen una serie de razones para escoger BGP (Border Gateway Protocol) como el protocolo para transportar las rutas VPNs, entre estas características mencionaremos, la posibilidad de BGP de soportar grandes listas de rutas y de transportar información adjuntada a las rutas como un atributo opcional de BGP, esta última posibilidad de BGP hace posible además la propagación de los RT entre los enrutadores PE.

Con lo anteriormente expuesto se resuelve el problema de que varias VPN puedan utilizar el mismo rango de direcciones IP en sus redes, pero recordemos que dentro de una misma VPN no pueden haber sitios que utilicen el mismo rango de direcciones IP, tampoco podemos entrelazar VPNs que utilicen los mismos rangos de direcciones en sus redes. Este problema de solapamiento de direcciones IP ocurre también en los escenarios de redes IP estándar donde si es necesario una interconexión total entre sitios los rangos de direcciones han de ser únicos o desarrollar NAT.

Con la intención de ilustrar el intercambio de los protocolos de enrutamiento por VPNs con el MP-BGP usado en el núcleo de la red del SP, se considera el caso de la Empresa A en la red, se asume que el sitio-1 en el PE1 utiliza OSPF para interactuar con el backbone, el sitio-2 no utiliza protocolos de enrutamiento, es configurado con rutas estáticas y que el sitio-3 utiliza RIP (Routing Information Protocol). Lo mencionado anteriormente se muestra en la figura 2.23.

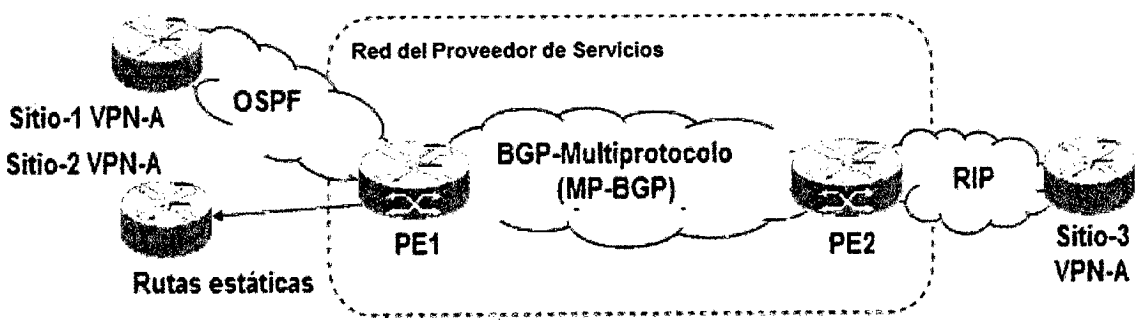


Figura 2.23 Protocolos de Enrutamiento usados en la VPN-A. (Gómez & Moliner, 2005)

La información de enrutamiento colectada por varios protocolos de enrutamiento, así como las rutas estáticas configuradas en el enrutador PE1 son redistribuidas dentro de MP-BGP, las direcciones son aumentadas con el RD en el momento de la redistribución

y las rutas exportan las RT especificadas en los VRF origen, también adjuntadas. La información de enrutamiento resultante de 96 bits es propagada por MP-BGP hasta el enrutador PE2. El enrutador PE2 después de recibir las rutas a través de MP-BGP inserta las rutas recibidas en varias tablas VRF, basándose en el RT adjuntado a cada ruta individual. El RD es eliminado de los 96 bits cuando la ruta es insertada dentro del VRF, terminando nuevamente como un enrutamiento IP tradicional, por último la información de enrutamiento recibida a través de BGP es redistribuida dentro de procesos RIP y transmitida al sitio-3 al RIP realizar actualizaciones.

2.2.2.3.3 Propagación de rutas VPNV4 en una MPLS VPN

Las VRFs separan las rutas de cliente en los nodos PE, pero absolutamente todos los prefijos son transportados a través de la red MPLS. Potencialmente pueden ser cientos de miles de rutas ya que pueden ser numerosas las VPNs de cliente configuradas. Para este transporte de rutas, BGP es el protocolo ideal ya que está probado y es estable para el manejo de grandes tablas de rutas, por eso es el protocolo estandarizado para internet. Gracias a la transformación de prefijos IP en prefijos VPNv4 (RD + prefijo IP), todas las rutas se pueden transportar de manera segura a través de la red.

El nodo PE recibe rutas IP desde el CE mediante un IGP o mediante eBGP. Estas rutas IP de una VPN determinada se insertan en una tabla de rutas VRF. Esta VRF depende de la que esté configurada sobre el interfaz del PE que conecta con el CE que inyecta las rutas. Estas rutas IP se convierten en rutas VPNv4 una vez que los prefijos se asignan al RD correspondiente, es entonces cuando entran en el proceso de MP-BGP. BGP se encarga de distribuir estas rutas VPNv4 hacia todos los PEs en esa VPN. El que la ruta VPNv4, después de separarse del RD, sea puesta en la tabla de VRF como rutas IP o no depende de si los RTs permiten la importación a esa VRF. Esas rutas IP son entonces anunciadas al router CE mediante un IGP o eBGP que esté corriendo entre el PE y el CE.

Para comprender todos estos procesos, en la siguiente ilustración se ven los pasos que se establecen para que se produzca comunicación IP entre dos CEs a través de una VPN MPLS.

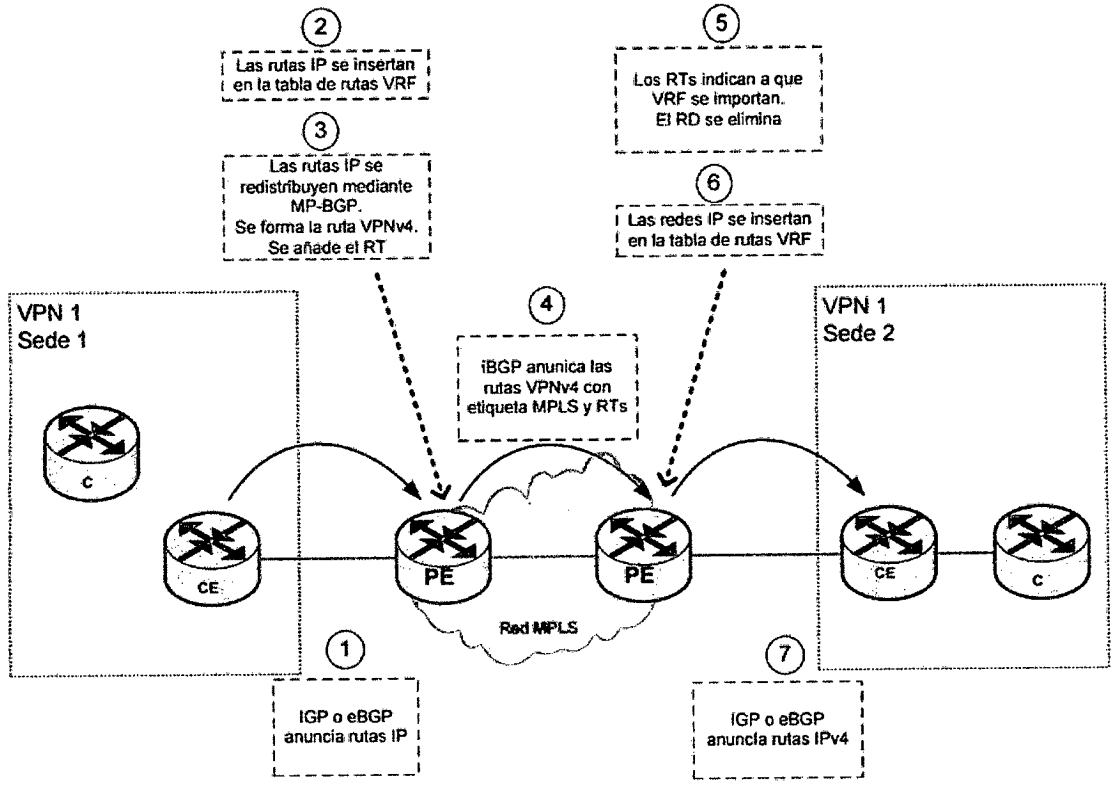


Figura 2.24 Propagación de rutas en una VPN MPLS paso a paso. (González Carrasco, 2011)

2.2.2.3.4 Envío de paquetes en una VPN

En el envío de paquetes utilizando MPLS, cada paquete es etiquetado a la entrada del dominio MPLS con una etiqueta que identifica el punto de salida del dominio MPLS, con esta etiqueta es enviado a través de la red; todos los enrutadores del núcleo de la red conmutan las etiquetas sin necesidad de conocer la cabecera IP. Ahora cuando un enrutador PE (salida de un dominio MPLS) recibe un paquete de una VPN, este paquete no tiene información de su VPN destino. Para lograr que la comunicación entre sitios de una VPN sea única un segundo nivel de etiquetas debe ser incorporado.

Cada enrutador PE asigna una etiqueta única para cada ruta en cada instancia de Enrutamiento y Envío VPN (VRF). Estas etiquetas son propagadas conjuntamente con las correspondientes rutas a través del MP-BGP hasta todos los routers PE. Los routers PE reciben las actualizaciones MP-BGP e instalan las rutas recibidas en sus tablas VRF, también instalan las etiquetas VPN asignadas por los routers PE en sus tablas VRF, con lo anterior expuesto la red MPLS/VPN está lista para el envió de paquetes VPN. Cuando un paquete VPN es recibido por un router PE (entrada al dominio MPLS), es

examinado el VRF que le corresponde y la etiqueta asociada con la dirección destino por el router PE (salida del dominio MPLS) es buscada. Otra etiqueta orientada hacia el router PE (salida) es obtenida desde la tabla de envío global. Ambas etiquetas son combinadas en la pila de etiquetas, y adjuntadas en la delantera del paquete VPN, luego son enviadas hacia el router PE (salida).

Todos los enrutadores P en la red conmutan los paquetes VPN basados solamente en la primera etiqueta de la pila, las que apuntan al router PE (salida). En las reglas normales del envío en MPLS los routers P nunca analizan más allá de la primera etiqueta y son así completamente ajenos a la segunda etiqueta y los paquetes transportados por la red. Los routers PE (salida) reciben los paquetes etiquetados con la segunda etiqueta las cuales únicamente identifican la VRF destino y en algunas ocasiones la interface de salida en el router PE. Un análisis es ejecutado en el VRF y el paquete es enviado hacia el adecuado enrutador frontera del cliente (CE).

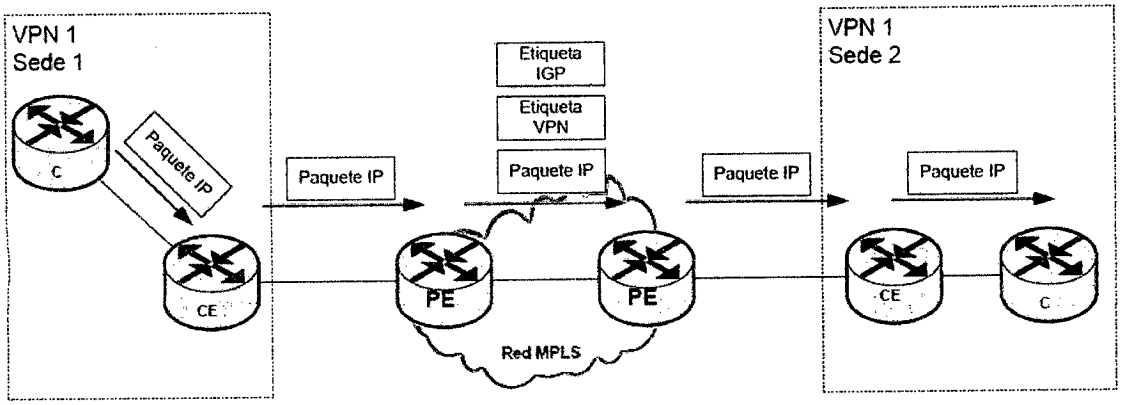


Figura 2.25 Formato de paquetes en una red VPN MPLS. (González Carrasco, 2011)

2.3 Comunicación entre múltiples proveedores de servicios (Inter-AS MPLS VPNs)

Nuestra descripción de la arquitectura MPLS VPN hasta ahora ha asumido que todos los sitios de los clientes VPN están conectados a un solo proveedor de servicios a través de enlaces entre los router PE y routers CE, y sin ningún tipo de intercambio directo de información de enrutamiento entre las instalaciones del cliente.

También hemos puesto hincapié el hecho de que un cliente puede optar por utilizar el servicio MPLS VPN para conectar sus sedes porque resulta una forma más escalable de proporcionar conectividad VPN en comparación con los métodos tradicionales, como

los modelos overlay o peer-to-peer. Sin embargo, es posible que el cliente tenga sedes dispersas en una amplia zona geográfica, (abarcando en muchos casos, varios países), por lo que se hace necesaria la conexión entre múltiples proveedores de servicios para poder brindar el servicio VPN requerido.

La nueva arquitectura MPLS-VPN se puede entender como arquitecturas Inter-provider (Inter proveedores) o Multi-provider (Múltiples proveedores). Donde cada segmento de red bajo la administración un proveedor de servicios, se conoce como Sistema Autónomo. Una red Inter-AS MPLS VPN ofrece los siguientes beneficios:

- Permite que una VPN pueda atravesar la red troncal de diferentes proveedores de servicios VPN.
- Los proveedores de servicios que ejecutan sistemas autónomos independientes pueden ofrecer conjuntamente servicios de MPLS VPN al mismo cliente. Una VPN puede comenzar en un sitio del cliente y atravesar diferentes proveedores de servicios VPN antes de llegar al otro sitio del mismo cliente. Anteriormente, MPLS VPN podía atravesar solamente la red troncal BGP del proveedor. Esta nueva arquitectura permite que múltiples sistemas autónomos puedan formar una red continua, entre los sitios de los clientes de un proveedor de servicios.
- Permite que una VPN pueda existir en diferentes áreas geográficas
- Un proveedor de servicios puede crear una VPN en diferentes áreas geográficas. Tener todo el flujo de tráfico de su VPN a través de un punto (entre las zonas) le permite un mejor control de la tasa de tráfico de la red entre las zonas.

En la figura 2.26 se muestra un esquema general de un escenario que requiere implementar Inter-AS MPLS-VPN.

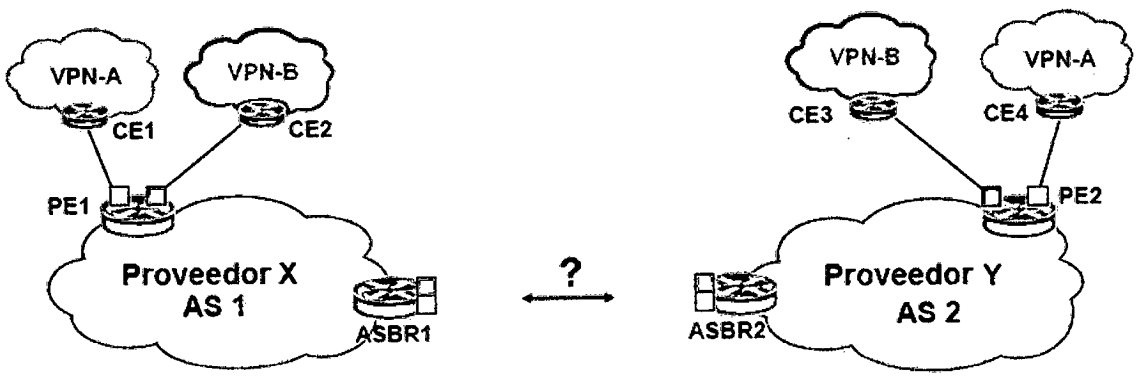


Figura 2.26 Esquema de una red Inter-AS MPLS-VPN. (Hass, 2005)

2.3.1 Modelos Inter-AS MPLS- VPNS

Existen cuatro maneras diferentes de construir una INTER-AS MPLS- VPNS. La necesidad de implementar una red INTER-AS MPLS- VPNS suele ocurrir cuando dos sitios del mismo cliente son proporcionados por diferentes proveedores. En este caso, ambos proveedores de servicios necesitan ponerse de acuerdo sobre la manera de interconectar sus VPNs (Virtual Private Networks) con el fin de proporcionar la conectividad de extremo a extremo para el cliente.

Otra situación típica es cuando un ISP que brinda el servicio de suministro de VPNs es comprado por uno más grande. En este caso, a pesar de que es el mismo ISP, todavía tiene dos redes diferentes con dos sistemas autónomos (AS) diferentes. A fin de proporcionar conectividad VPN de extremo a extremo, se implementan cuatro modelos INTER-AS MPLS- VPNS. Los tres primeros son los más comunes, y el último es una mezcla. (Huertas, 2012)

- Opción 10A: Back to Back VRF
- Opción 10B: MP-eBGP entre ASBRs
- Opción 10C: Multihop MP-eBGP entre Route-Reflectors (RRs)
- Opción AB: una mezcla mejorada de las opciones A y B y desarrollado por Cisco.

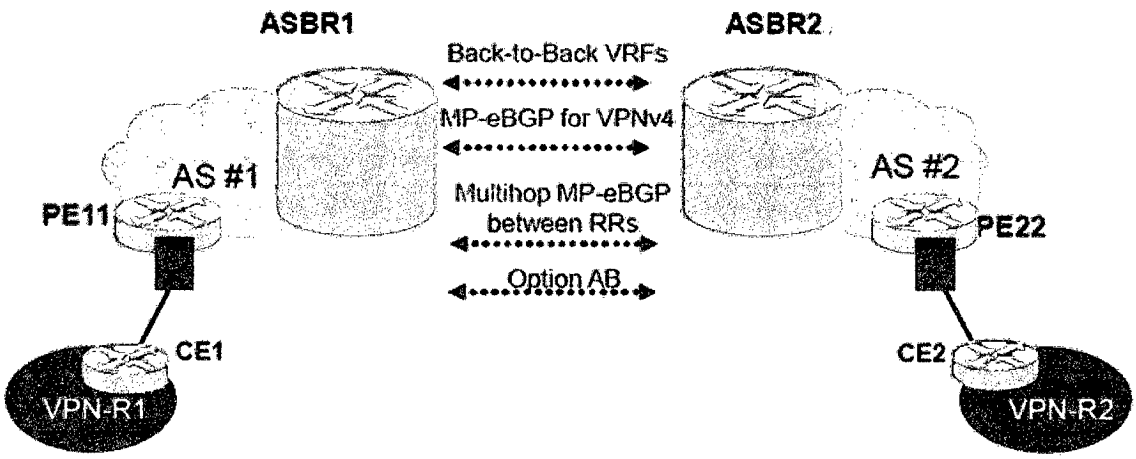


Figura 2.27 Sitios VPN unidos a diferentes proveedores de servicios de MPLS VPN (Kollar, 2009)

2.3.1.1. INTER-AS MPLS VPN—OPTION 10A: Back-to-Back VRFs (Mahmoud, 2008)

Este modelo llamado VRF-to-VRF (como se indica en la documentación RFC 4364) o back-to-back VRF (como es nombrado por Cisco) es el modelo más simple para permitir Inter-AS MPLS VPN entre diferentes proveedores.

Los routers que interconectan los sistemas autónomos de los proveedores funcionan como routers de borde (ASBRs), y se encuentran interconectados a través de un único enlace que consiste en subinterfaces lógicas o por medio de múltiples enlaces físicos. En cada ASBR se configuran las VRFs para recoger las rutas VPN del cliente, y cada subinterfaz o interfaz conectada entre los ASBRs se asocia a una sola VRF del cliente. Los paquetes se envían como paquetes IP puros entre los ASBRs, y cualquier protocolo de enrutamiento PE-CE se pueden utilizar con el fin de anunciar el uno al otro la dirección involucrada en la VPN.

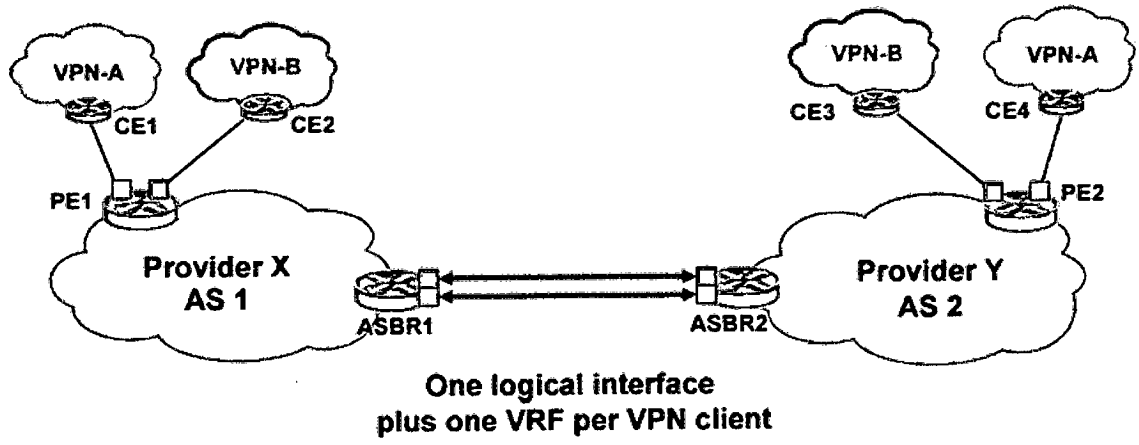


Figura 2.28 Back-to-Back VRFs. (Hass, 2005)

En cada VRF se puede configurar cualquier protocolo de enrutamiento dinámico (eBGP, RIPv2, EIGRP, OSP), o enrutamiento estático para distribuir las rutas de VPN a su par adyacente. Sin embargo, el uso de eBGP es el más usado debido a que mejores mecanismos de política, escalabilidad y seguridad. Cada ASBR trata el ASBR vecino como una CE, y e intercambian las rutas rutas IPv4 por VRF de la misma manera que lo hacen un PE y un CE.

Esta opción es la solución más fácil de implementar una Inter-AS MPLS VPN, aunque no es escalable porque hay que configurar todos los VRFs en los ASBRs. Por otra parte, es muy seguro para los proveedores de Internet, ya que no necesitan ninguna IGP, LDP

o interacción MP-BGP entre sí.Sólo tienen que conectarse entre sí con una interfaz física y hacer tantas sub-interfaces como VPNs que desean conectarse, y luego utilizar un protocolo de enrutamiento PE-CE (podría ser rutas estáticas) con el fin de intercambiar información de enrutamiento VPN.

2.3.1.2 INTER-AS VPN—OPTION 10B: MP-eBGP entre ASBRs (Mahmoud, 2008)

En este opción no hay necesidad de tener que configurar las VRFs por cada cliente en los ASBRs como fue el caso en la opción 10A, en este método se intercambian prefijos VPNv4 para diferenciar los clientes VPN. Los ASBRs utilizan MP-eBGP entre sí para transportar las rutas VPNv4 entre los sistemas autónomos, y los paquetes VPN se transportan como paquetes etiquetados entre los ASBRs, a diferencia de la opción 10A.

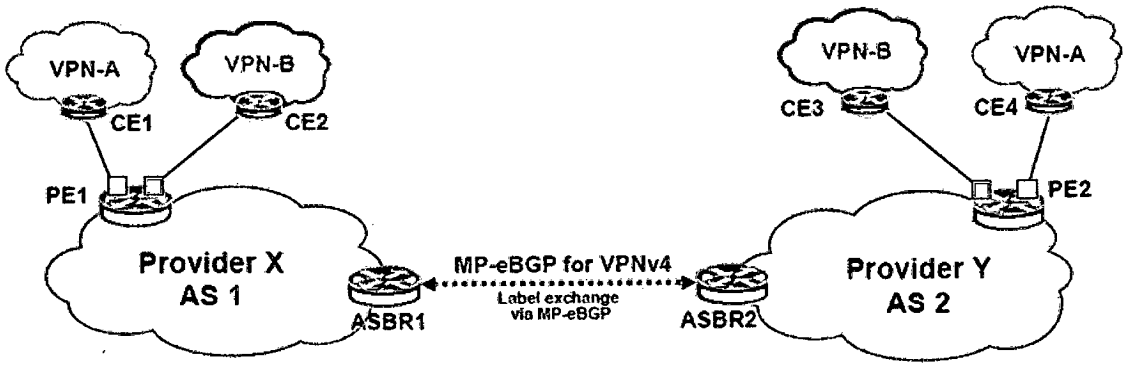


Figura 2.29 MP-eBGP entre ASBRs. (Hass, 2005)

El principal problema de esta opción se presenta en la calidad de servicio (QoS) y la garantía de entrega de extremo a extremo (concretamente entre las ASBRs) ya que el tráfico de todos los clientes es atravesado por un único enlace como paquetes etiquetados, y muy probablemente este enlace tenga limitada capacidad de ancho de banda.

En toda red MPLS VPN, el reenvío de paquetes se lleva a cabo sólo si el router especificado como el siguiente salto BGP en la actualización de BGP entrante es el mismo router que asignó la etiqueta de VPN en la cabecera MPLS VPN. Sin embargo, cuando las VPNs están dispersas y atraviesan más de un proveedor, el siguiente salto es cambiado cuando existe una sesión eBGP entre los ASBRs y por lo tanto una etiqueta

VPN se asigna en los ASBRs cada vez que el siguiente salto es cambiado. Al igual que la opción back-to-back VRF, el LSP termine en el ASBR que anuncia la ruta, y éste tiene que asignar una nueva etiqueta para dicha ruta antes de enviarla a través de un mensaje MP-eBGP a su ASBR vecino.

Por defecto un router PE descarta prefijos VPNv4 entrantes que no son importados a ninguna de las VRFs que tiene configuradas localmente, entonces, los ASBRs que no tienen VRFs configuradas deben configurarse para que puedan aceptar los prefijos BGP VPNv4 de los routers de borde dentro del sistema autónomo.

Este modelo tiene tres subopciones: 2a (Next-hop-self), 2b (Redistribute connected) y 2c (Multi-hop MP-eBGP), que difieren principalmente en la forma como se establece la sesión MP-eBGP entre los ASBRs. Las dos primeras subopciones (2a y 2b) utilizan las interfaces físicas directamente conectadas, mientras que la subopción 2c establece la sesión MP- eBGP mediante interfaces loopback.

2.3.1.2.1 Subopción 2a – Método Next-hop-self

En esta opción, la sesión MP-eBGP se establece entre las interfaces físicas directamente conectadas. Con el enfoque del Next-hop-self, cada ASBR debe anunciarse a sí mismo como el siguiente salto de la ruta MP-eBGP recibida por el ASBRs vecino cuando publica la ruta dentro de su propio sistema autónomo a través de MP-iBGP. Cada vez que el siguiente salto cambia, una nueva etiqueta se anuncia para el prefijo BGP.

2.3.1.2.2 Subopción 2b – Método Redistribute connected

En este método, la etiqueta MPLS VPN cambia solamente una vez en el ASBR local cuando publica las rutas VPNv4 al ASBR remoto, y cuya etiqueta no será modificada por el ASBR remoto. Cada ASBR debe hacer que la dirección del siguiente salto del ASBR vecino sea alcanzable para su propio sistema autónomo y así ya no sea necesario que se anuncie a sí mismo como el siguiente salto de la ruta.

En otras palabras, el ASBR acepta la ruta sin cambiar el siguiente salto ni la etiqueta, que continúan siendo los del ASBR remoto. Lo que se hace en su lugar es redistribuir

las redes directamente conectadas dentro del IGP para anunciar el siguiente salto de las rutas recibidas desde el ASBR remoto.

En el caso de los subopciones 2a y 2b, no hay necesidad de habilitar TDP/LDP o algún IGP entre los ASBRs. La sesión MP-eBGP que se establece en su lugar permite a las interfaces involucradas transmitir paquetes etiquetados, pues ambos ASBRs conocen las etiquetas VPN.

2.3.1.2.3 Subopción 2c – Método Multi-hop MP-eBGP

En esta subopción, la sesión MP-eBGP entre los ASBRs se hace utilizando las IPs loopback en lugar de las interfaces físicas, utilizando para ello MP-eBGP Multisalto. En primer lugar hay que configurar estáticamente las direcciones IPs loopback como el siguiente salto en cada ASBR. Se puede también usar tanto el método "next-hop-self" como redistribute connected o redistribute stati, debido a que el siguiente salto en el AS vecino es una ruta estática hacia la loopback, dentro del IGP en cada ASBR.

La subopción 2c es utilizada principalmente cuando existen múltiples enlaces entre los ASBRs, con la finalidad de balancear carga para incrementar el ancho de banda disponible. A diferencia de las subopciones anteriores, aquí si se tiene que habilitar LDP entre los ASBRs debido a que ahora los vecinos MP-eBGP no se ecuentran directamente conectados.

La desventaja de esta subopción, está en la forma como los LSRs generan e insertan etiquetas para rutas estáticas. Además, esto varía significativamente si las interfaces que conectan los ASBRs son multiacceso o punto-punto.

Si las interfaces son multiacceso, la ruta estática debe apuntar a la dirección IP del siguiente salto y no a la interfaz de salida. De lo contrario, la etiqueta saliente será nula y todo el etiquetado local será nulo. El ASBR hará una búsqueda local de la IP y descartará el paquete, por lo tanto cuando se utilizan interfaces de multiacceso en una red MPLS VPN, nunca las rutas estáticas deben apuntar a las interfaces de salida. Si las interfaces son punto-punto, entonces no habrá problemas debido a que el LSR local tendrá una etiqueta saliente sin importar como esté configurada la ruta estática.

2.3.1.3 INTER-AS MPLS VPN—OPTION 10C: Multihop MP-eBGP entre Route-Reflectors (RRs) (Mahmoud, 2008)

Esta opción se considera que es la más escalable, ya que en comparación con la opción 10B , los ASBRs no necesitan aprender todos los prefijos VPNv4, debido a que ahora la sesión MP-eBGP se establece entre los routers Route Reflector (RRs), y no en los ASBRs. Los ASBRs serán los responsables únicamente de intercambiar las direcciones del siguiente salto IPv4 juntos con sus etiquetas a través de eBGP, completándose así la creación de un LSP desde el PE de ingreso local hasta el PE de egreso remoto.

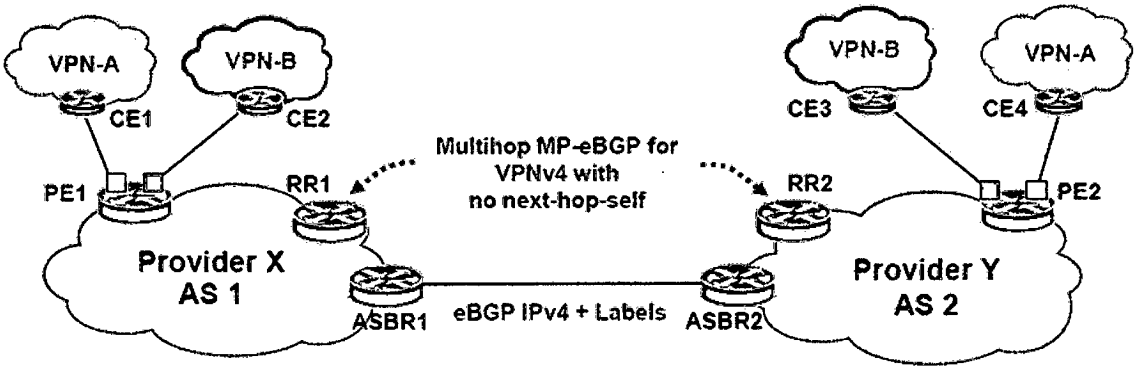


Figura 2.30 Multihop MP-eBGP entre Route-Reflectors (RRs). (Hass, 2005)

En cada ASBR se debe habilitar la sesión eBGP para permitir el intercambio de etiquetas MPLS junto con las rutas IPv4. Para la sesión MP-eBGP entre los Route Reflector (RRs), se debe hacer que el siguiente salto no sea modificado cuando las rutas VPNv4 se intercambien entre los RRs, y los prefijos VPNv4 tampoco deben modificarse. Este es el único caso en el que el LSP no es dividido y la etiqueta MPLS-VPN original es usada en todo el tramo, pues el siguiente salto en la ruta VPNv4 nunca cambia.

Debido a que cada AS puede alcanzar los siguientes saltos internos del AS vecino, la seguridad hace que ésta sea una alternativa viable cuando los AS se encuentran bajo una misma autoridad, como es el caso de un proveedor con AS en diferentes regiones del mundo. Sin embargo, se puede incrementar la seguridad utilizando métodos de encriptación para que el tráfico esté cifrado.

2.3.1.4 INTER-AS MPLS VPN—OPTION AB (Mahmoud, 2008)

Esta opción combina los mejores aspectos de las opciones 10A y 10B. Recordemos que la desventaja de la primera opción es que se necesita una sesión BGP para cada subinterfaz (y al menos una subinterfaz para cada VPN), que causa problemas de escalabilidad, ya que la red crece. En la segunda opción la desventaja es que, debido a que el tráfico es MPLS, no se puede aplicar mecanismos de calidad de servicio QoS para el tráfico IP y las VRFs no pueden aislarse.

La opción AB permite que los diferentes sistemas autónomos se puedan interconectar mediante el uso de una sola sesión MP-BGP en la tabla de enrutamiento global para transportar tráfico del plano de control. Esta sesión MP-eBGP señala los prefijos VPN entre los dos ASBRs para cada enrutamiento virtual y reenvío VRF. El tráfico de plano de datos está en una interfaz VRF. Este tráfico puede ser o bien IP o MPLS.

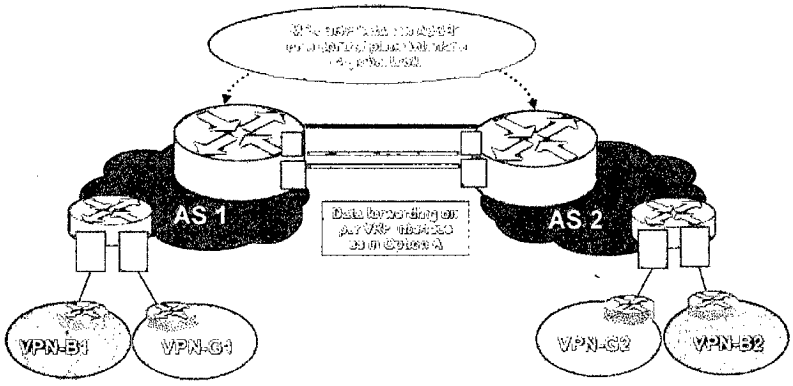


Figura 2.31 Opción AB. (Kollar, 2005)

2.3.2 BGP y Sistemas Autónomos (AS)

2.3.2.1 Autonomous System Number (ASN)

Los Sistemas Autónomos se comunican entre sí mediante routers, los que intercambian información para tener actualizadas sus tablas de ruteo mediante el protocolo BGP (Border Gateway Protocol) e intercambian el tráfico de Internet que va de una red a la otra. A su vez cada Sistema Autónomo es como una Internet en pequeño, ya que su rol se llevaba a cabo por una sola entidad, típicamente un Proveedor de Servicio de Internet (ISP) o una gran organización con conexiones independientes a múltiples redes, las cuales se apegaban a una sola y clara política de definición de trayectorias La nueva definición RFC 19301 fue necesaria debido a que múltiples organizaciones podían utilizar BGP con números de AS privados con un ISP que conecta a todas estas organizaciones a Internet. Aún considerando que el ISP podía soportar múltiples sistemas autónomos, Internet solo considera la política de definición de trayectorias establecida por el ISP. Por lo tanto, el ISP debería contar con un ASN registrado.

2.3.2.2 ASN en Perú

ASN	Nombre	Adyacencias v4	Rutas v4	Adyacencias v6	Rutas v6
AS28032	INTERNEXA PERU S.A	12	42	4	10
AS12252	AMERICA MOVIL PERU S.A.C.	10	183	3	2
AS3132	RED CIENTIFICA PERUANA	9	15	1	2
AS262182	MEDIA NETWORKS LATIN AMERICA SAC	9	33	9	24
AS6147	TELEFONICA DEL PERU S.A.A.	5	1,038	2	47
AS27843	OPTICAL TECHNOLOGIES S.A.C.	4	123	2	2
AS262253	ECONOCABLE MEDIA SAC	4	35	1	1
AS19180	AMERICATEL PERU S.A.	4	54	1	1
AS262168	COLINANET SRL.	3	3	0	0
AS22411	WIGO S.A.	3	13	0	0
AS52461	MOCHE INVERSIONES S.A.	2	5	0	0
AS52400	OLO DEL PERU S.A.C	2	2	0	0
AS28102	BANCO AZTECA PERU	2	1	0	0
AS27809	ALIGNET S.A.C	2	1	0	0
AS263224	EMPRESA DE TELECOMUNICACIONES MULTIMEDIA ALFA	2	4	0	0
AS262210	VIETTEL PER S.A.C.	2	43	0	0
AS21575	ENTEL PERU S.A.	2	41	0	0
AS61482	CONVERGIA	1	3	0	0
AS52278	FRAVATEL EIRL	1	1	0	0
AS27791	UNIVERSIDAD RICARDO PALMA	1	1	0	0
AS263692	DIRECTV PERU S.R.L	1	4	1	1
AS263229	NAP PERU	1	1	0	0
AS263189	GLG PERU SAC	1	5	0	0
AS263185	MEDIA COMMERCE PER S.A.C	1	1	0	0
AS262235	NETLINE PERU SA	1	8	0	0
AS26136	THE AMERICAN SCHOOL OF LIMA	1	1	0	0

Tabla 2.7 Número de ASN en Perú. (http://bgp.he.net/country/PE)

2.3.2.3 Sistemas Autónomos (AS)

Los Sistemas autónomos presentan las siguientes características:

- Cada AS está identificado por un número único denominado ASN (Autonomous System Number).
- Los ASN están delegados por IANA (Internet Asigned Number Authority) a los RIR (Regional Internet Registries) por bloques.
- Cada RIR asigna un ASN a cada organización.
- Hasta 2007 los ASN eran un número de 16 bits. Ahora se ofrecen de 32 bits, aunque no todos los sistemas son compatibles con la nueva numeración.
- Los ASN del 65512 al 65534 están reservados para uso privado y no pueden anunciarse en Internet.
- A partir del 1 de Enero de 2009 al solicitar un Sistema Autónomo (AS) a RIPE se asigna por defecto un AS de 32 bits (hasta ahora los AS eran de 16 bits), aunque se nos permite solicitar también ASs de 16 bits hasta el 1 de Enero de 2011.

2.3.2.3.1 Tipos

- **Multihomed** - Está conectado a más de un AS, de manera que puede permanecer conectado a Internet en el caso de fallo de una de las conexiones.
- **Stub** - Sólo está conectado a otro AS.
- **Transit** - Proporciona conexión entre distintos AS. (ISP)

2.3.2.4 ISP vs AS

Un ISP es una entidad administrativa que puede tener uno o más ASN asignados dependiendo de su arquitectura y distribución geográfica. En general, un ASN se puede asignar a un ISP pero también a una red corporativa. Por lo tanto no todos los AS son ISP, pero todos los ISP deben tener uno o mas ASN asignados.

2.3.2.5 BGP (Border Gateway Protocol)

Las características básicas de BGP son:

• Es un protocolo de encaminamiento externo que permite crear rutas entre sistemas autónomos (AS). En cada AS puede operar cualquier encaminamiento interno tipo RIP u OSPF.

• Un router que tiene un proceso BGP activo se llama BGP speaker. Para poder intercambiar información de encaminamiento BGP, dos routers vecinos (dos BGP speakers) deben establecer una sesión BGP a través del puerto 179 de TCP. En este caso estos dos routers se llaman peers o neighbors.

• BGP es un protocolo de tipo path vector. Es decir BGP recae en la categoría general de los protocolos vector distancia como RIP donde la mejor ruta es la que tiene menos saltos hasta el destino. BGP tiene pero algunos mecanismos adicionales. La información de encaminamiento BGP es una secuencia de números que identifican los diferentes ASes que hay que atravesar para llegar a un AS destino. Esta información evita la creación de bucles en las rutas. BGP además permite crear políticas de encaminamiento a través de una serie de atributos.

• Un As puede ser de tipo stub, multihomed o de transito. Stub cuando un AS tiene una única sesión BGP abierta con otro AS y solo recibe y transmite su tráfico. Multihomed en el caso que un AS tenga mas de un AS conectado por BGP (por si uno falla) pero no deja que trafico de un AS pase por el con destino otro AS. De transito cuando el AS proporciona servicio de transito entre dos ASes.

• Una sesión BGP que conecta dos routers de dos AS distintos se llama BGP externo (eBGP). En el caso que el AS sea de transito, los routers del AS que mantienen un eBGP deben tambien establecer una sesión BGP entre ellos, llamada BGP interna (iBGP), para que estos puedan redistribuir la información BGP entre los ASes.

• Hay cuatro tipos de mensajes BGP: open, update, keepalive y notification. open se utiliza para el establecimiento de la sesión BGP; update cuando hay una modificación de una ruta o se ha encontrado una nueva ruta; periódicamente dos routers vecino se envían mensajes de keepalive para para verificar que la sesión BGP sigue activa; notification notifica el cierre de una sesión BGP debido a algún error.

CAPÍTULO 3

PARAMETROS Y HERRAMIENTAS

3.1 Parámetros de medición para evaluar el rendimiento de una red

Para analizar el rendimiento de una red, se deben tomar en cuenta los siguientes parámetros, que son los que permiten caracterizarla.

3.1.1 Ancho de Banda

El ancho de banda (throughput) puede definirse como la tasa de paquetes por segundo enviados por una red multiplicado por la longitud del paquete, es decir, es la cantidad de datos digitales, medidos en bits o Bytes que un nodo o enlace de comunicaciones es capaz de transmitir por unidad de tiempo, medido en segundos. Es esta forma, las unidades de ancho de banda son el bps (bits por segundo) o Bps (Bytes por segundo) o múltiplos de estas cantidades. El ancho de banda de un enlace de comunicaciones depende de las características físicas de los dispositivos y de la técnica utilizada para modular los datos.

3.1.2 Retardo

El retardo (delay) es el tiempo medido en milisegundos, que tarda un paquete en viajar a través de una red como consecuencia del ancho de banda disponible, el tiempo de propagación de la señal a través de los enlaces de comunicaciones y el tiempo de procesado de datos en los nodos de red.

3.1.3 Jitter

El jitter es la variación de tiempo, medida en milisegundos, entre la llegada de dos paquetes consecutivos, como consecuencia de la política de gestión de red que es utilizada en los diferentes nodos de red para soportar el tráfico de ráfagas y permitir la agregación de flujos de datos. Es conocido también como variación del retardo.

3.1.4 Tasa de Pérdidas

La tasa de pérdidas es la relación que se establece entre los paquetes enviados y los paquetes recibidos. Ya que como consecuencia de errores de transmisión en los enlaces

de las redes y la congestión en los nodos de red se producen pérdidas de paquetes de datos. Comúnmente se expresa en porcentaje de paquetes perdidos.

3.1.5 Uso del CPU

Existen funciones críticas en los dispositivos de red, como el procesamiento de protocolos de enrutamiento y de conmutación de paquetes que requieren alto procesamiento. Estos procesos son llevados a cabo en la memoria y comparten el CPU. Si el uso del CPU es muy alto, es posible que una actualización de ruta no sea realizada o que un paquete sea descartado.

3.1.6 Tiempo de convergencia

Es el tiempo que le toma a la red establecer las sesiones necesarias, intercambiar información y actualizar sus tablas de enrutamiento. Esto es importante para determinar cuánto demorará una red en recuperarse ante un corte o caída de uno o más enlaces.

3.2 Herramientas de desarrollo

Para realizar el análisis de la red, se han utilizado una serie de aplicaciones que se describen a continuación. Todas ellas son software libre y se pueden encontrar de manera gratuita en internet.

3.2.1 GNS3

GNS3 es un software simulador de redes, creado por Jeremy Grossman, Benjamin Marsili, Claire Godjil, Alexey Eromenko y lanzado en el mes de Octubre 2007. Este Software es parte del Conocido Freeware, su licencia no tiene costo y se encuentra fácilmente en la web. Se basa en un simulador grafico en el que se pueden crear topologías de red, desde las más básicas hasta las más complejas.

En él se puede emular routers Cisco, así como servidores Linux y sus conexiones físicas, por medio de los diferentes tipos de cables, desde los Ethernet, FastEthernet, Gigabit Ethernet, etc. Resulta una herramienta extremadamente útil, que nos sirve para emular la red completa, sus conexiones y realizar troubleshooting para determinar los inconvenientes presentados.

Además, el GNS3 tiene una aplicación complementaria llamada Dynamips que sirve para ejecutar el IOS de los equipos Cisco directamente en los routers simulados que

vamos a utilizar lo que nos permite realizar las configuraciones exactamente igual a como las haríamos en los equipos físicos, conectando un cable de consola, y usando un programa terminal. También cuenta con compatibilidad a otras aplicaciones de simulación como el VirtualBox que permite emular tráfico de VoIP, para habilitar este tipo de redes en el programa.

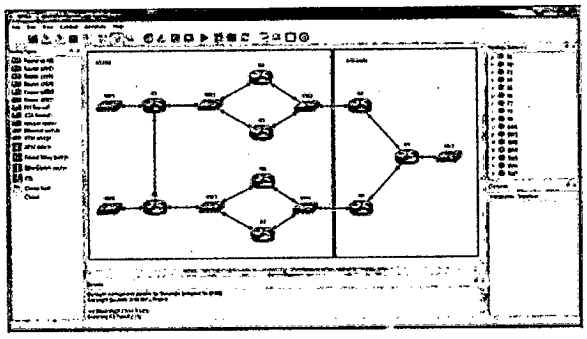


Figura 3.1 Captura de la pantalla del GNS3 (Martínez, 2008)

3.2.2 .IPERF

Iperf es una herramienta que permite analizar el rendimiento de una red. Soporta tráfico UDP y TCP. Proporciona el ancho de banda máximo en TCP. Permite establecer varios parámetros y características de UDP. Luego reporta ancho de variación del retardo (jitter) y pérdida de paquetes. Esta herramienta funciona de manera cliente-servidor. En la figura 3.2 se muestra captura de una prueba en el cliente y en la figura 3.3 una captura de la pantalla del servidor.

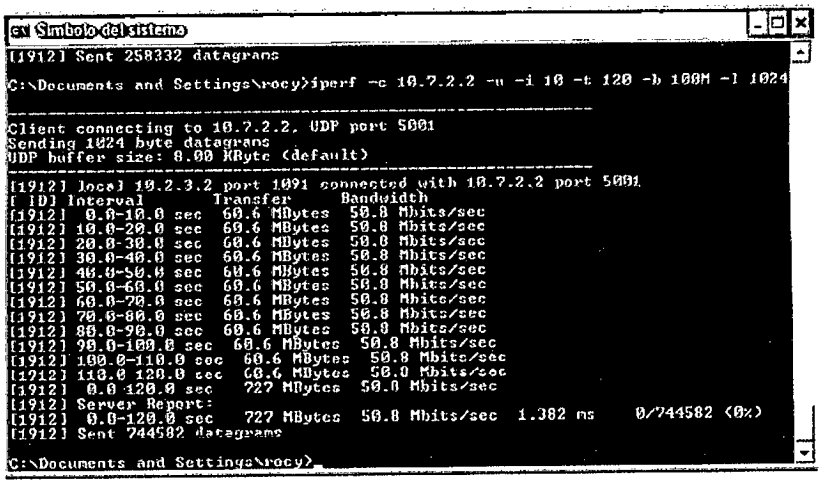


Figura 3.2 Captura de la pantalla de Iperf actuando como cliente (Martínez, 2008)

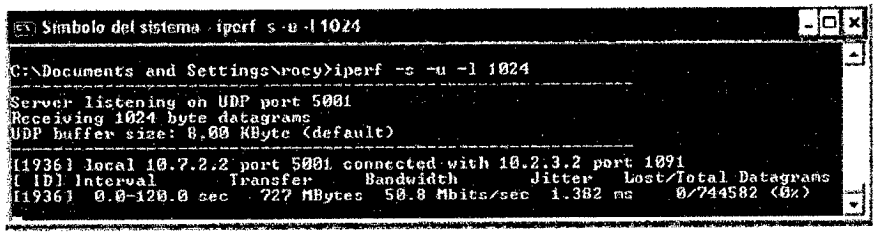


Figura 3.3 Captura de la pantalla de Iperf actuando como servidor (Martínez, 2008)

Las características más relevantes de herramienta Iperf son las siguientes:

- TCP:
  - Medida de ancho de banda
  - Reporta tamaño de MTU y tamaños leídos
  - Soporte para tamaño de ventana TCP vía socket buffers.
  - El cliente y el servidor pueden tener múltiples conexiones simultáneas

- UDP:
  - El cliente puede crear flujos UDP con determinado ancho de banda.
  - Medida de pérdida de paquetes
  - Medida de jitter
  - Capacidad de multicast
  - Puede correrse por un tiempo específico en vez de por cantidad de datos transferidos.
  - Selecciona la mejor unidad para el tamaño de los datos que se están reportando.
  - El servidor maneja múltiples conexiones, en vez de retirarse luego de una simple prueba.
  - Imprime reportes de ancho de banda promedio, jitter y pérdida de paquetes en intervalos específicos
  - Usa flujos representativos para probar como la compresión de la capa de enlace afecta el ancho de banda disponible.

3.2.3 WIRESHARK

Wireshark, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos. Tiene una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red, estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red en funcionamiento o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix, Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows. En la figura 3.4 podemos ver un ejemplo de captura de paquetes por wireshark.

Las características más relevantes de la herramienta Wireshark son las siguientes:

- Mantenido bajo la licencia GPL.
- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Basado en la librería pcap.
- Tiene una interfaz muy flexible.
- Grandes capacidades de filtrado.
- Admite el formato estándar de archivos tcpdump.
- Reconstrucción de sesiones TCP.
- Se ejecuta en más de 20 plataformas.
- Es compatible con más de 480 protocolos.
- Puede leer archivos de captura de más de 20 productos.

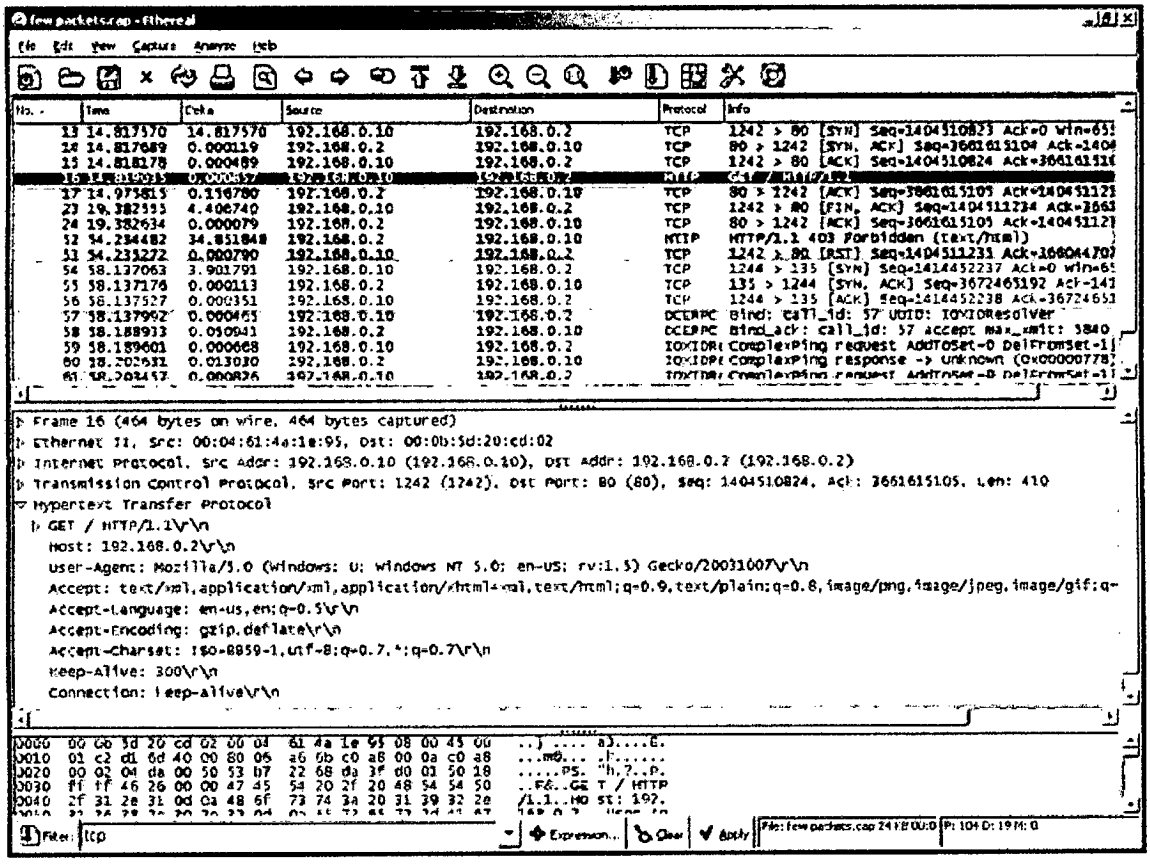


Figura 3.4 Captura de la pantalla del Wireshark (Martínez, 2008)

3.2.4 VLC

Es un software de código abierto multiplataforma desarrollado por la organización VideoLan, el cual puede desempeñar funciones tanto de cliente como servidor. Soporta varios métodos de compresión en audio y video y permite transmitir contenido usando unicast o multicast. Cuenta con un diseño modular lo que permite incluir extensiones de manera ordenada y sencilla para el soporte de nuevos formato de archivos, codecs y formas de transmisión. Entre las muchas extensiones con las que cuenta VLC se encuentra el NPAPI que permite a los usuarios ver archivos embebidos en sitios web sin usar softwares adicionales.

En la figura 2.6 se puede apreciar la interfaz gráfica del VLC y algunas de las opciones con las que cuenta.

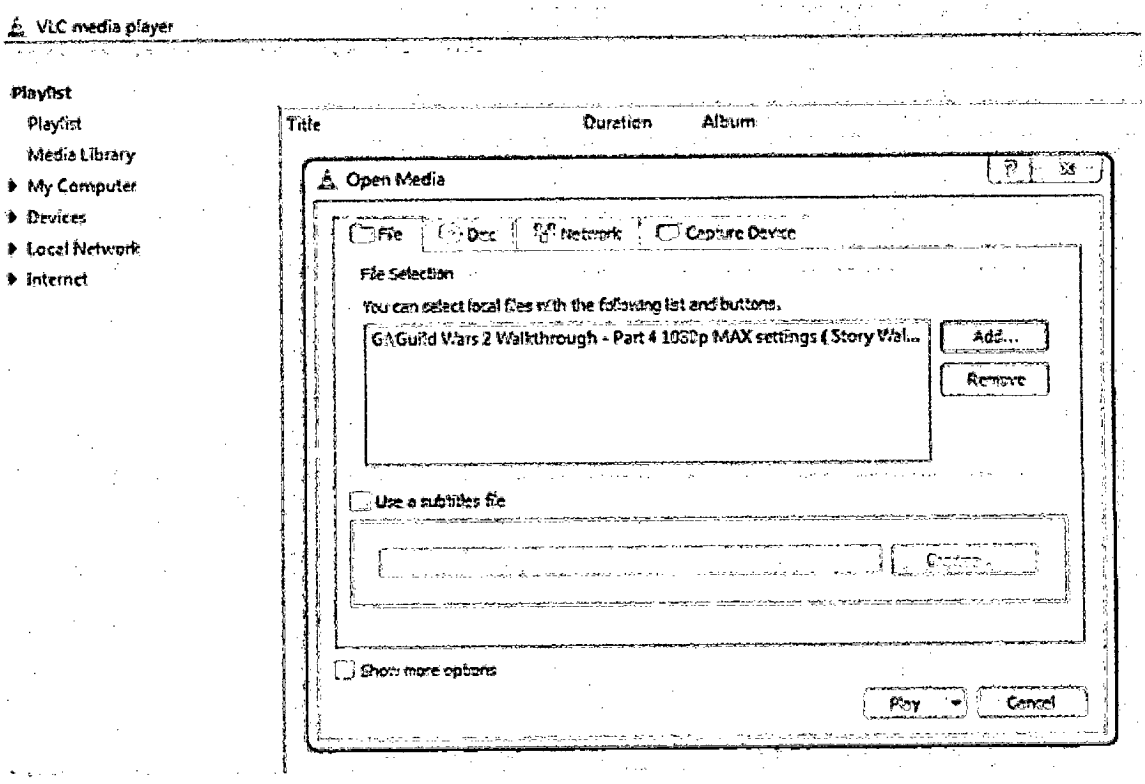


Figura 3.5 Interfaz gráfica de VLC (Calderón, 2014)

3.2.5 Estadísticas del router

Se utilizarán los comandos que muestren el uso total del CPU del equipo durante un periodo de tiempo. El uso máximo es medido y registrado cada segundo, y el promedio de uso es calculado en un periodo de tiempo de alrededor de un minuto.

CAPÍTULO 4

INGENIERÍA DEL PROYECTO

4.1 Pruebas de desempeño

4.1.1 Principios de simulación

Como se propone en esta Tesis, el objetivo principal es brindar la propuesta técnica que permita la comunicación de una red MPLS-VPNs entre múltiples proveedores de servicios. La elección de la propuesta técnica se basará en las pruebas de comparación de los diferentes modelos Inter-AS MPLS VPN realizadas en este capítulo. Cabe

recalcar que, a pesar de que las pruebas a realizarse serán simuladas, la comparación no pierde valor ya que muchas instituciones y centros de investigación basan sus estudios en diferentes simuladores.

El estudio de los diferentes modelos Inter-AS MPLS VPN se basa principalmente en la forma en la que se establece la interconexión entre los proveedores, por lo que las mediciones se realizarán principalmente en estos enlaces, es decir, en entre los routers ASBR. Además, se realizarán mediciones extremo-extremo. La arquitectura de red interna de cada uno de los proveedores es transparente para este estudio, y se implementarán de tal forma que ambas sean simétricas.

Para determinar las ventajas y desventajas de estos modelos, se empleará la herramienta de simulación GNS3 el cual es un simulador de red que permite la emulación de redes complejas. Actualmente, se ha convertido en una herramienta muy popular en la comunidad científica e instituciones de la industria de las telecomunicaciones ya que permite el diseño y estudio de diferentes arquitecturas y aplicaciones permitiendo gran flexibilidad para las pruebas de diferentes soluciones.

Por otro lado, los parámetros tomados en cuenta durante las pruebas de comparación realizadas, serán los propuestos en el capítulo anterior.

4.1.2 Simulación

En esta sección, se detallan las topologías implementadas y las pruebas de simulación realizadas con los diferentes modelos Inter-AS MPLS VPN. Se muestran imágenes de los gestores de la red que permiten ver parte de las pruebas hechas. Los resultados consolidados se encuentran en un cuadro resumen al final de cada sección.

4.1.2.1 Modelo 1: Back-to-Back VRFs

En la topología que se muestra en la figura 4.1 se ha considerado un total de 8 routers y dos host uno de origen y el otro de destino ubicados en los extremos de la red. Cada router ejecuta como sistema operativo el IOS de cisco 7200 elegidos porque estos ofrecen la capacidad de ejecutar MPLS y el protocolo BGP.

Los routers PE1, P1-AS1 y PE2 pertenecen al proveedor con sistema autónomo 1 (AS1), mientras que los routers PE3, P1-AS2 y PE4 pertenecen al proveedor con sistema autónomo 2 (AS2). Como se observa se tiene un cliente con dos sedes remotas (Sede 1 y 2) cada sede tiene sus redes LAN establecidas, el cliente requiere tener conexión entre sus sucursales a través de las redes de diferentes proveedores de servicios. En cada router del cliente (CE1 y CE2) se configurara la VPN cliente.

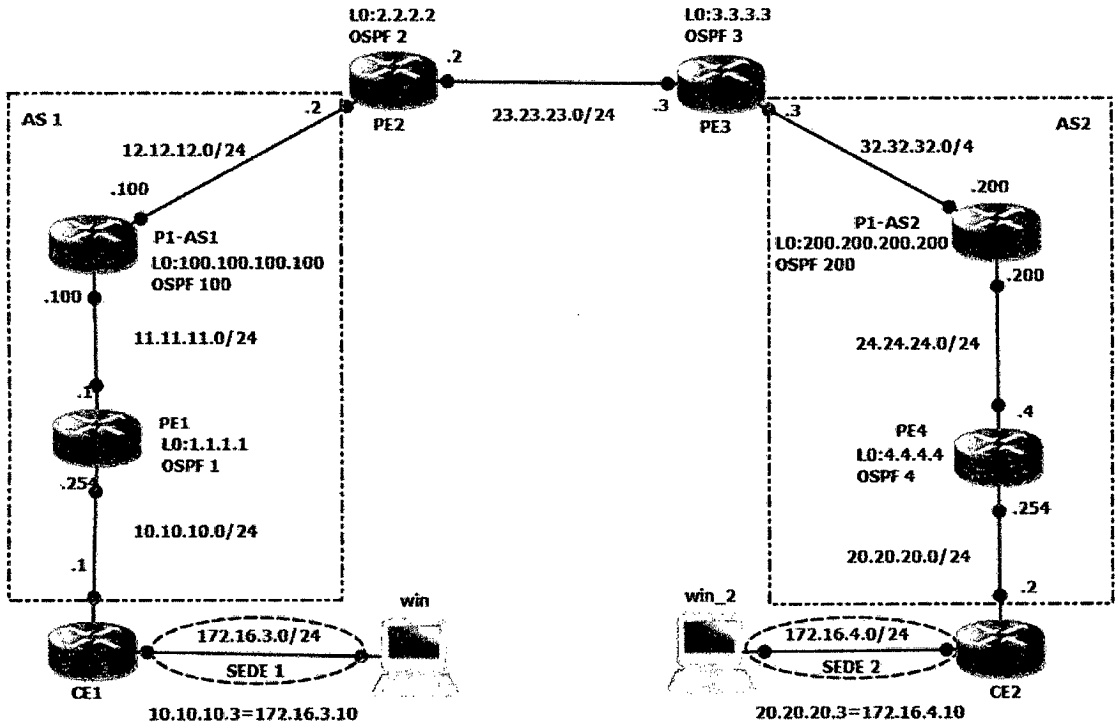


Figura 4.1 Topología de simulación del modelo 1 - Back-to-Back VRFs (Elaboración Propia)

El proveedor 1 usa BGP AS 1 y el proveedor 2 usa BGP AS2. El router PE2 y el router PE3 pueden ser conectados con una única interfaz o subinterfaces. Las interfaces están asociadas con una VRF dada (VRF BLUE para ambos proveedores, aclarar que ambos pueden ser diferentes nombres). El enrutamiento convencional es configurado entre sitios MPLS VPN para distribuir rutas IPV4 a sus peers (al otro nombre VRF). Sin embargo, el router ASBR PE2 trata al otro router de borde PE3 como si fuera un router CE1 o CE2; similar caso ocurre del router PE3 a PE2. Este enfoque permite usar backbone MPLS VPN; sin embargom también introduce una gran complejidad porque requiere enlaces dedicados para cada VPN entre las adyacencias de PE2 y PE3. La información de enrutamiento VPN es pasada entre los dos routers (PE2 y PE3) como si fuera simplemente un formato IPv4.

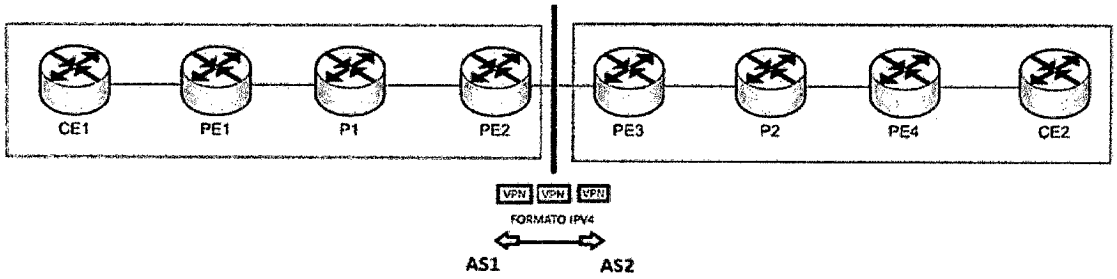


Figura 4.2 Esquema del modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Pruebas de conexión extremo-extremo

Una vez tenemos configurado todo el escenario, debemos comprobar que funciona la conexión extremo-extremo en ambos sentidos. Se entiende como conexión extremo-extremo aquella que va desde el host "origen" al host "destino" pasando a través de la red de los dos proveedores de servicios.

Para ello enviaremos una serie de paquetes ICMP (Internet Control Message Protocol), o sea, pings a través de la red, con un número de repeticiones de 200 y 500 desde la PC1 a PC2 y en simultáneo desde PC2 a PC1, ver figura 4.3 con 200 repeticiones y figura 4.4 con 500 repeticiones.

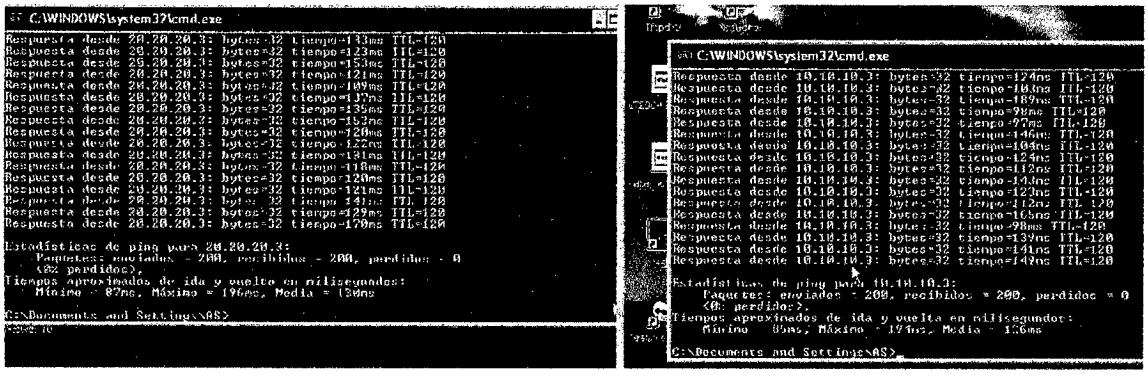


Figura 4.3 Ping con 200 repeticiones en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Podemos observar cómo se han recibido los paquetes y ninguno se ha perdido, por lo tanto podemos confirmar que hay conectividad entre los equipos finales del cliente. Finalmente vamos a realizar la misma prueba pero con un numero de 500 repeticiones.

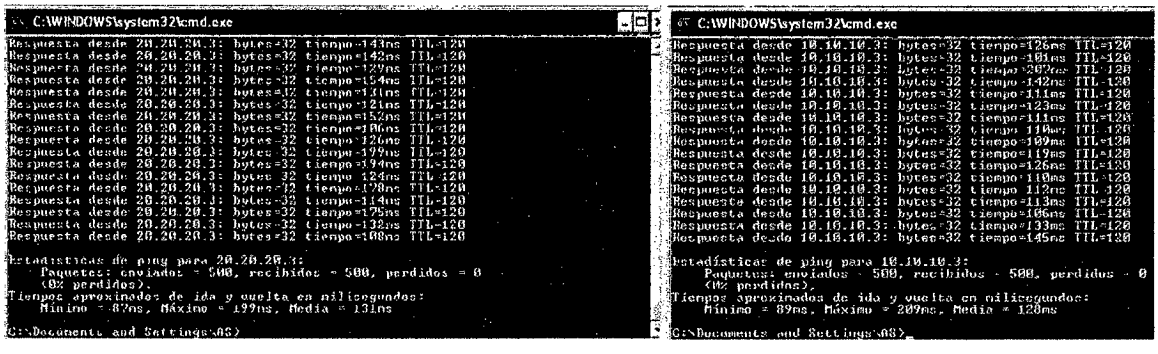


Figura 4.4 Ping con 500 repeticiones en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Igual que en el caso anterior la prueba de conexión ha sido un éxito. Los resultados de estas pruebas se muestran en la tabla 4.1.

Número de repeticiones	Retardo promedio de PC1 A PC2	Retardo promedio de PC2 A PC1
200	130 ms	126 ms
500	131 ms	128 ms

Tabla 4.1 Resultados de la conectividad entre las sedes del cliente en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Pruebas de medición del ancho de banda

Luego se realizó la medición del ancho de banda para este cliente con el enlace sin conexiones adicionales, con tráfico UDP a un enlace de 10Mbps. Para medir este parámetro se usó la herramienta Iperf.

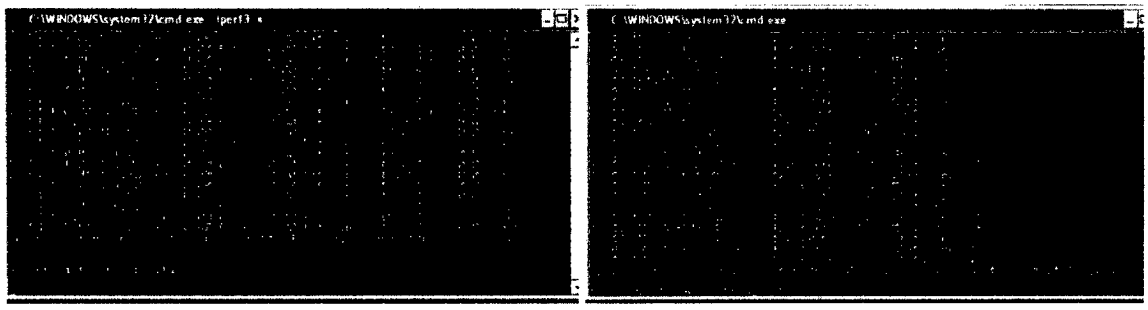


Figura 4.5 Ancho de banda a 10 Mbps en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

En la figura anterior se aprecia un ancho de banda para este cliente de 9.91 Mbps, que equivale a un rendimiento de 96.78%.

De forma similar se midió el ancho de banda para este cliente ahora con trafico UDP a un enlace de 20 Mbps, y se apreció un ancho de banda de 19.8 Mbps, que equivale a un rendimiento de 96.78%.

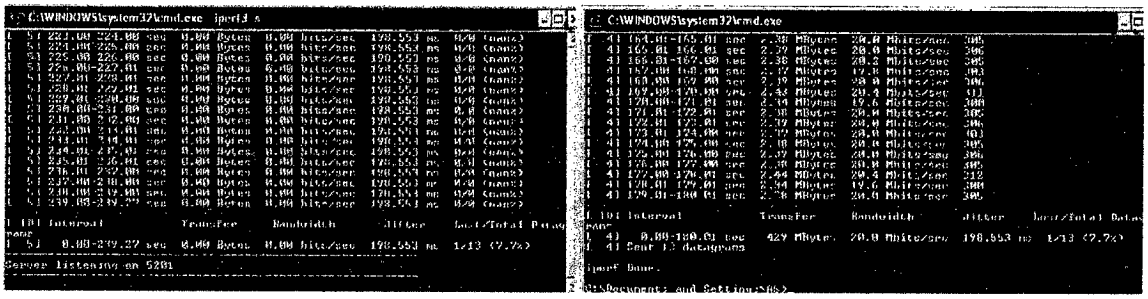


Figura 4.6 Ancho de banda a 20 Mbps en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Las dos pruebas sobre la red (10 y 20 Mbps) arrojaron los resultados mostrados en la tabla 4.2.

Ancho de banda (Mbps)	Ancho de banda obtenido (Mbps)	Jitter (ms)
10 Mbps	9.91	119.064
20 Mbps	20	198.553

Tabla 4.2 Resultados de pruebas del ancho en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Pruebas de medición del tiempo de convergencia

Para medir el tiempo de convergencia, se reinició dos veces la sesión BGP en el router PE2. En ese momento el sniffer conectado al router, que ya había iniciado la captura de tramas segundos antes, muestra las tramas BGP que anuncian las rutas. Ahora aquí encontramos la sesión de los vecinos 45.45.45.4 a 45.45.45.5, es decir, del router PE2 al router PE3.

Luego de la ejecución del comando "clear ip bgp" en PE2 y realizada la prueba, podemos decir que el modelo VRF – VRF es un modelo virtual, ya que el reseteo del proceso BGP en PE2 no produce ninguna comunicación alguna de un proceso BGP con PE3, ya que este modelo solamente comparte prefijos VPNv4, y comparte solamente mensajes de adyacencias BGP con el router PE1, ya que, éste router pertenece al sistema autónomo AS1, para ello vemos en la figura 4.7.

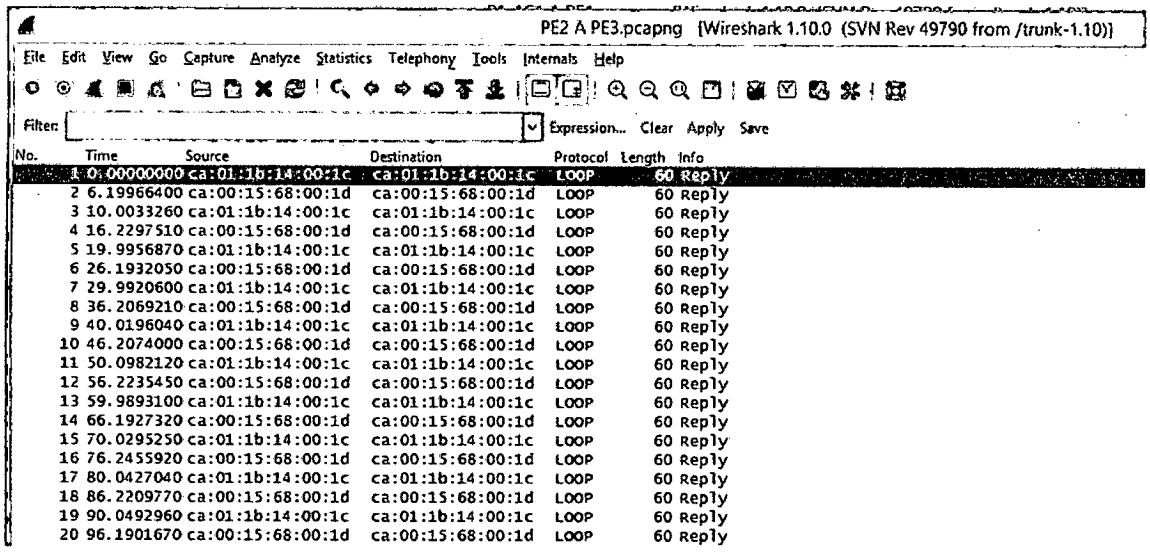


Figura 4.7 Mensajes entre los routers PE2 y PE3 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

El primer mensaje BGP OPEN de la sesión PE2 a P1-AS1 llega a los 65.492 segundos de iniciada la captura y anuncia el número 2.2.2.2 que identifica al router PE2. La figura 4.8 muestra dicha trama.

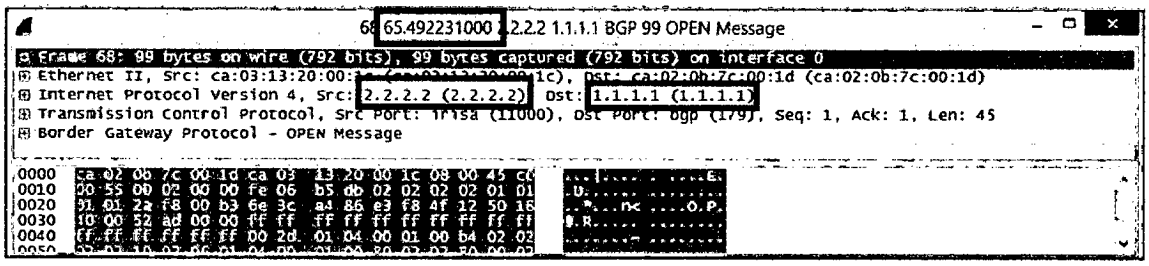


Figura 4.8 Primer mensaje BGP OPEN en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

De igual forma, para la sesión PE2 a P1-AS1 el último mensaje BGP UPDATE llega a los 99.661 segundos de iniciada la captura, vemos que el router PE2 entrega el mensaje update con una etiqueta 60 que es la etiqueta asignado por el router P1-AS1 tal como se muestra en la figura 4.9.

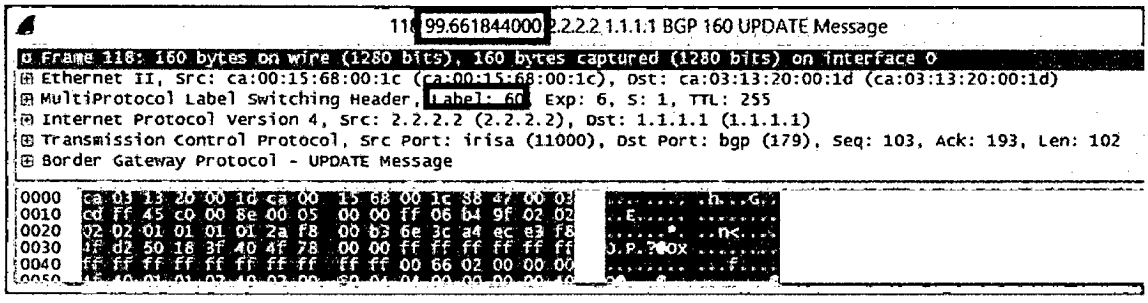


Figura 4.9 Ultimo mensaje BGP UPDATE en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

En la tabla 4.3, se muestran los resultados del tiempo de convergencia.

Mensaje BGP	Tiempo de llegada (s)
Open BGP	65.492
Update BGP	99.661
Tiempo de Convergencia	33.719

Tabla 4.3 Resultados de pruebas del tiempo de convergencia en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Lo cual tenemos una variación de tiempo de 33.179 segundos.

Pruebas del uso del CPU

Para la prueba de utilización del CPU del router, se reinició la sesión BGP en el router de borde PE2. Aquí utilizaremos el comando *show processes cpu history* en los vecinos del router mencionado.

En las siguientes imágenes se muestran los resultados obtenidos:

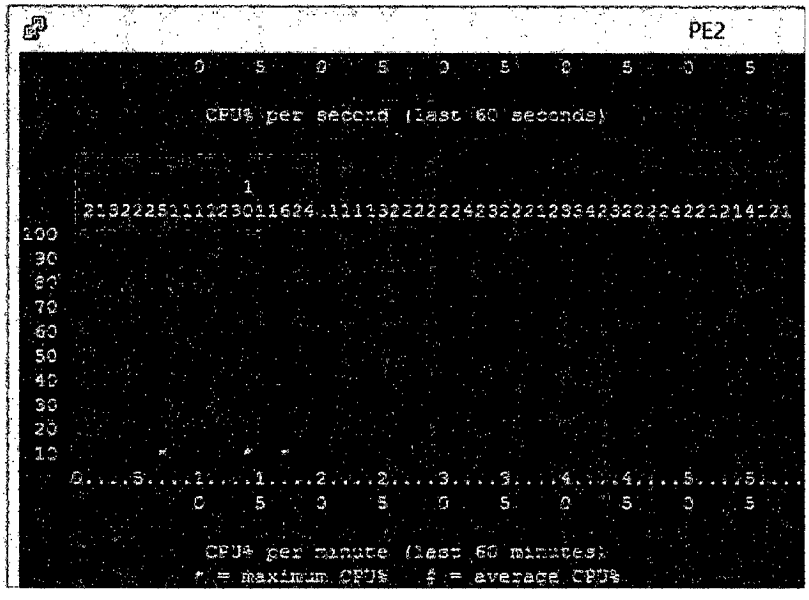


Figura 4.10 Uso del CPU con reinicio BGP en router PE2 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

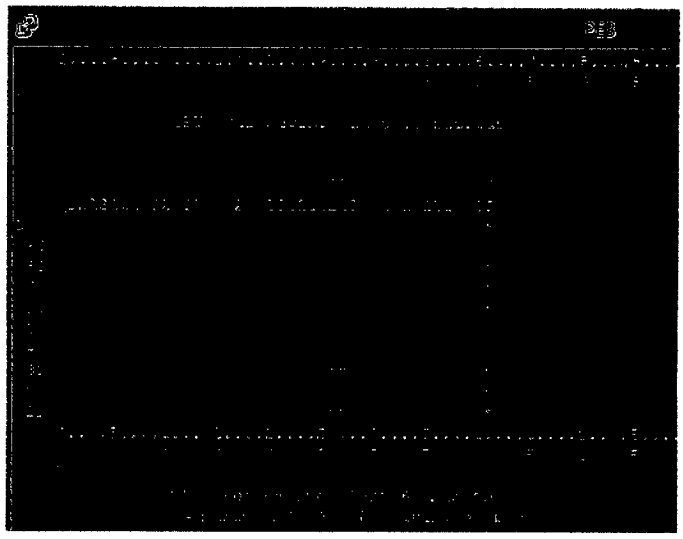


Figura 4.11 Uso del CPU con reinicio BGP en router PE3 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

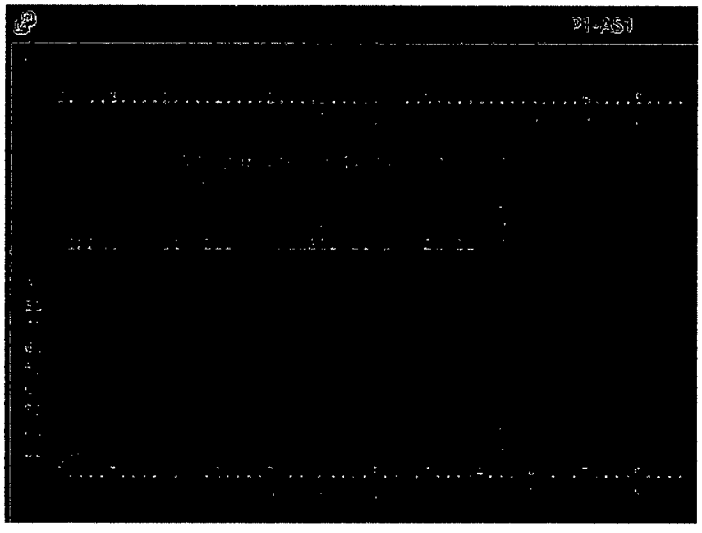


Figura 4.12 Uso del CPU con reinicio BGP en router P1-AS1 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

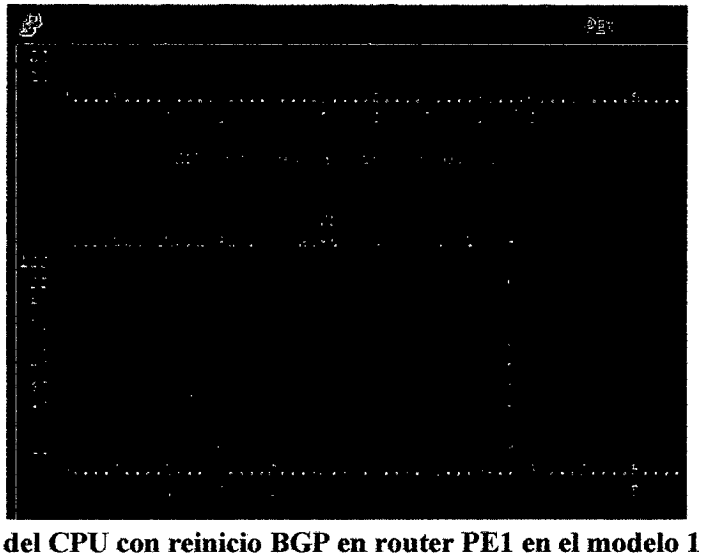


Figura 4.13 Uso del CPU con reinicio BGP en router PE1 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Donde observamos que para PE2 tiene una variación entre 3% y 5%, el router PE3 tiene un pico de 2%, pese a que es un router de borde del AS 2 y además como se explicó anteriormente, solamente es una ruta virtual, lo cual no varía mucho, ahora con P1-AS1 tiene un pico –casi nada- de 1 % y el router PE1 con 9%, lo cual se resume en la tabla 4.4.

Equipo	Valor máximo del uso del CPU
Router PE2	10 %
Router PE3	2 %
Router P1-AS1	1 %
Router PE1	9%

Tabla 4.4 Resultados del uso del CPU en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Análisis de la implentación del Modelo 1 - Back-to-Back VRFs.

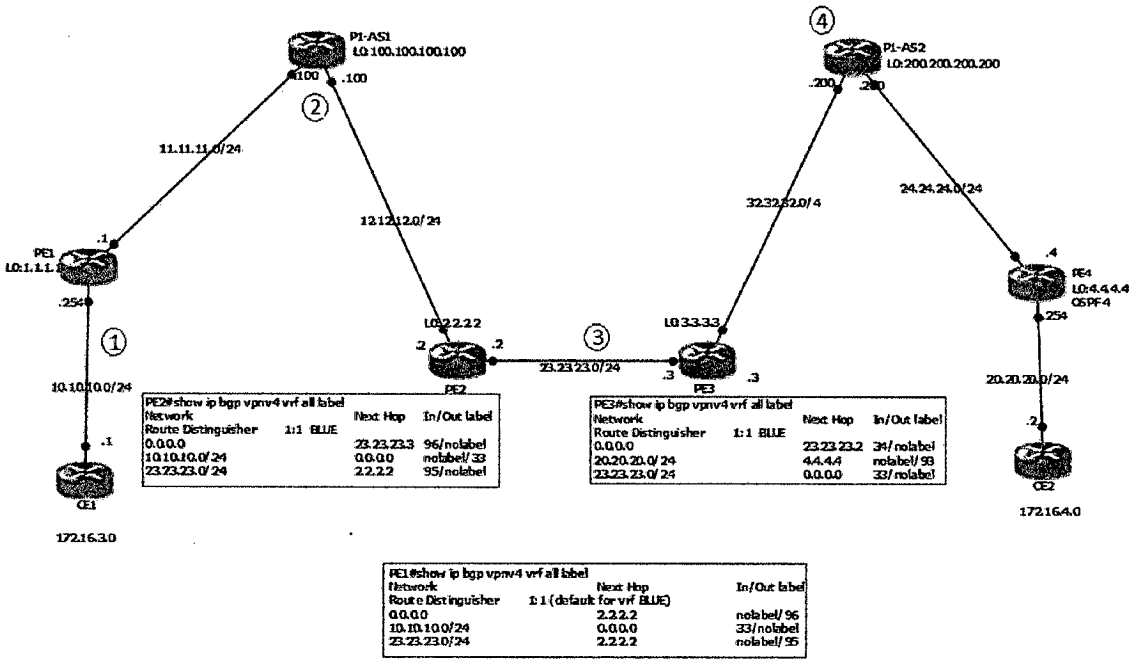


Figura 4.14 Implementación del modelo 1 - Back-to-Back VRFs (Elaboración Propia)

De la figura 4.14 se tiene que:

1. CE1 envía la red 10.10.10/24 como una actualización IPV4 a P1-AS1
2. P1-AS1 transforma la red 10.10.10.0/24 como una ruta VPNv4, localiza una etiqueta 33 VPNv4 y envía como una actualización VPNv4 con él mismo con un "next-hop".
3. PE2 acepta la red 10.10.10.0/24 en VRF BLUE para aceptar rutas con RT 1:1. Entonces traduce la actualización VPNv4 a IPV4 e inserta la ruta en BLUE; PE2 envía 10.10.10.0/24 como una actualización IPV4 a PE3. El router PE3 trata a

PE2 como un router parecido a CE1 y acepta la red 10.10.10.0/24 como una actualización de él.

4. CE2 envía la actualización IPV4 de la red 10.10.10.0/24 a PE4.

En la figura 4.15 tenemos la distribución de etiquetas y después el respectivo tracer del router CE1 a PC2 y el router CE2 a PC1.

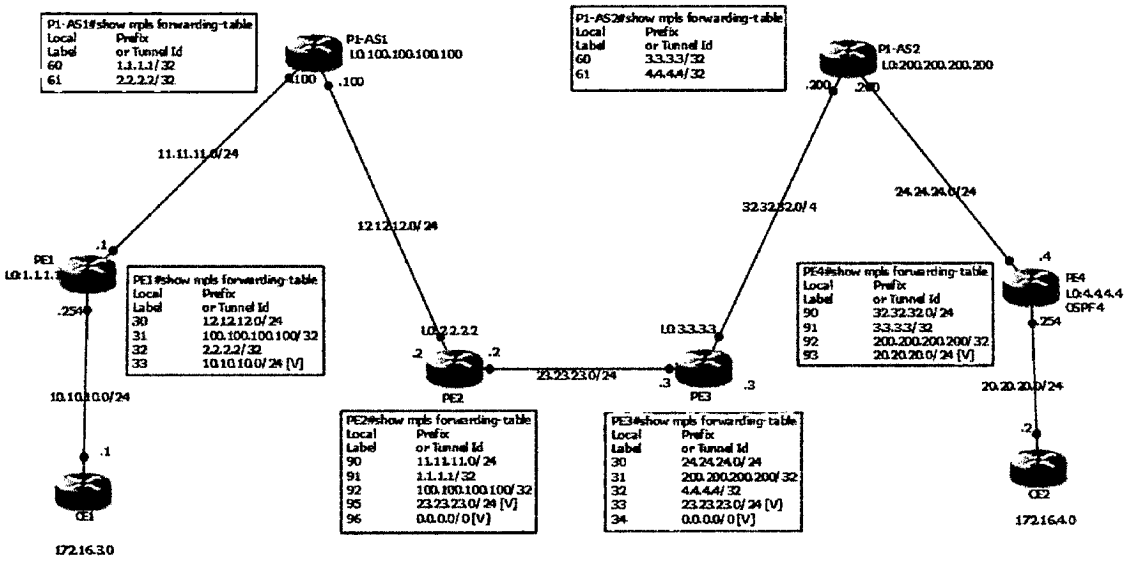


Figura 4.15 Distribución de etiquetas en la implementación del modelo 1 - Back-to-Back VRFs (Elaboración Propia)

Figura 4.16 Tracert exitoso entre el router CE1 al PC2 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

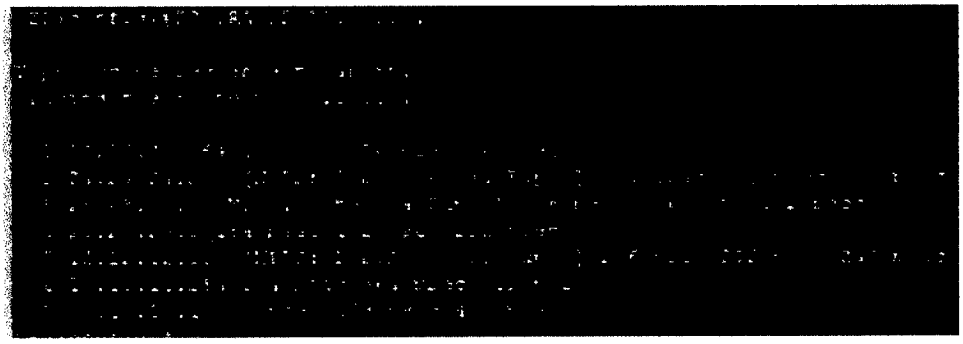


Figura 4.17 Tracert exitoso entre el router CE2 al PC1 en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

4.1.2.2 Modelo 2: MP-eBGP entre ASBRs - Next-hop-self

En la topología que se muestra en la figura 4.18 se ha considerado al igual que en el caso anterior un total de 8 routers y dos hosts, uno de origen y el otro de destino, ambos ubicados en los extremos de la red. En este modelo ya no hay necesidad de configurar las VRFs de cada cliente en los ASBRs de los proveedores (Routers PE2 y PE3), pues en su lugar los ASBRs usando MP-eBGP intercambian prefijos VPNv4 para diferenciar los clientes VPN.

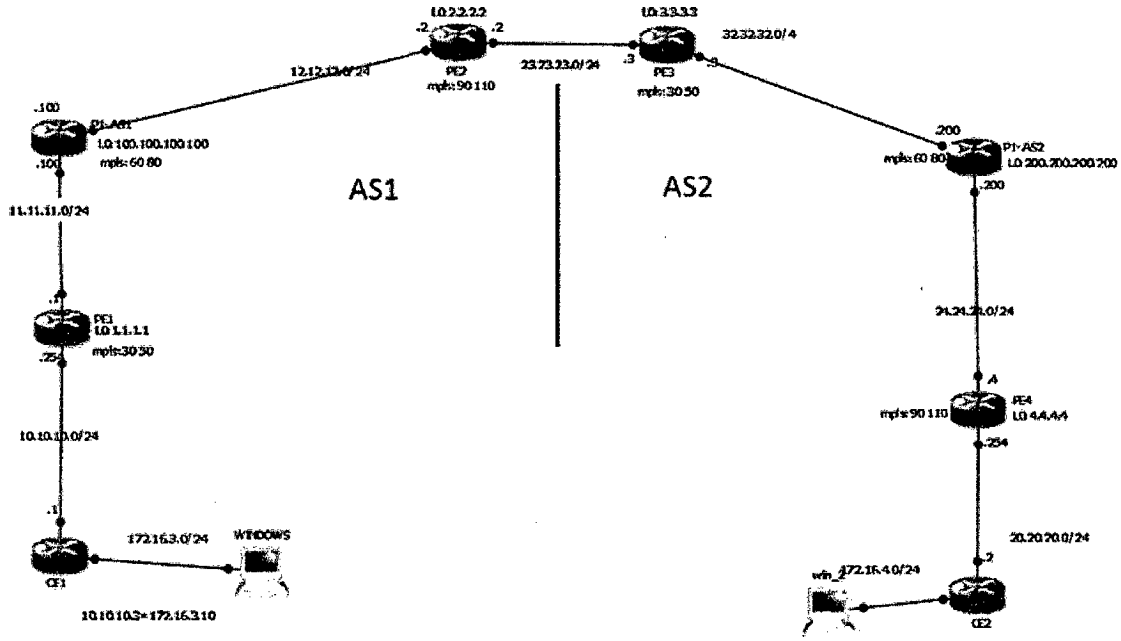


Figura 4.18 Topología de simulación del modelo 2 - MP-eBGP entre ASBRs - Next-hop-self (Elaboración Propia)

En este modelo, cuando la acción next-hop-self es usado, PE2 anuncia asimismo con el next hop para P1-AS1, y, similarmente, PE3 anuncia asimismo como next-hop a P1-AS2. Porque el next-hop es modificado, una nueva etiqueta VPNv4 ha sido generada. El router de borde eBGP PE2 distribuye la ruta a PE3 en la adyacencia del sistema autonomo, específicamente en su propia dirección como el nex-hop-eBGP, y asigna una nueva etiqueta VPNv4. Esta etiqueta es progagada a PE3.

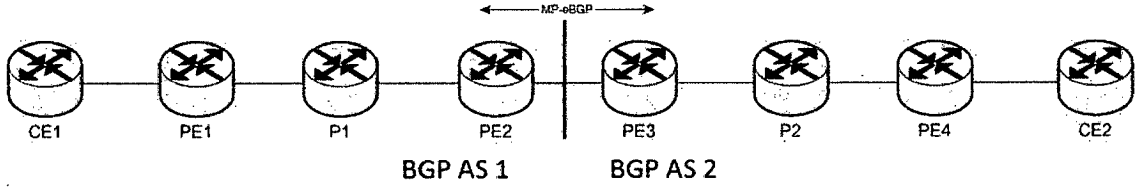


Figura 4.19 Esquema del modelo 2 - MP-eBGP entre ASBRs - Next-hop-self (Elaboración Propia)

El router PE3 recibe la ruta VPNv4 en la sesión MP-eBGP del router PE2. El next-hop-self es de nuevo usado y, como resultado, el next-hop es modificado desde el router PE2 al router PE3 cuando PE3 propagado estas rutas vía sesión MP-iBGP a P1-AS2. Porque el next-hop es modificado, la etiqueta VPN es modificada también y va a ser usada por el router PE3 para mapear el trafico entrante de PE4 en el LSP correcto hacia el router PE3.

Pruebas de conexión extremo-extremo

Para verificar la conectividad entre los equipos finales del cliente se realizó la acción ping con un número de repeticiones de 200 y 500 desde la PC1 a PC2 y en simultáneo desde PC2 a PC1, ver figura 4.20 con 200 repeticiones y figura 4.21 con 500 repeticiones.

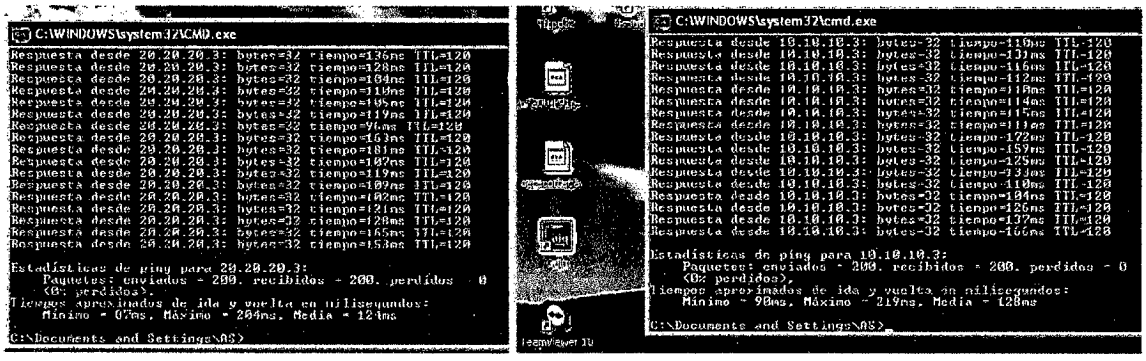


Figura 4.20 Ping con 200 repeticiones en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

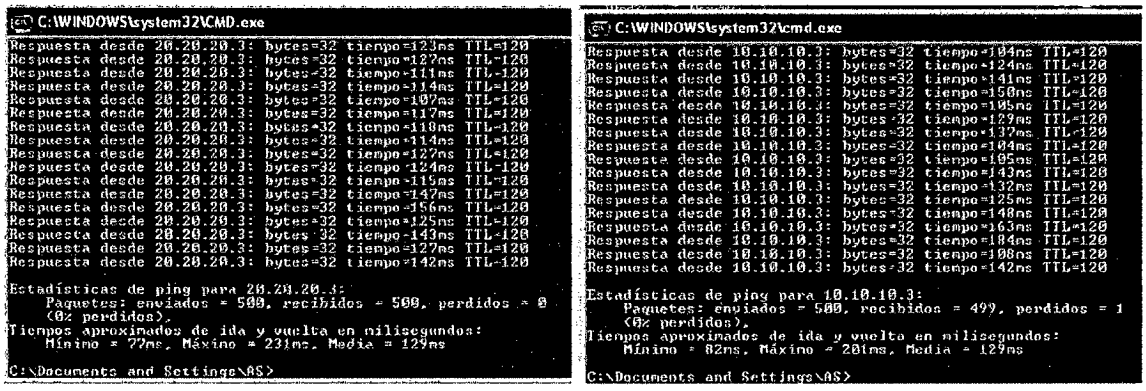


Figura 4.21 Ping con 500 repeticiones en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

Las pruebas de conexión fue un éxito y se logró conectividad entre los equipos finales del cliente. Los resultados de estas pruebas se muestran en la tabla 4.5.

Número de repeticiones	Retardo promedio de PC1 A PC2	Retardo promedio de PC2 A PC1
200	124 ms	128 ms
500	129 ms	129 ms

Tabla 4.5 Resultados de la conectividad entre las sedes del cliente en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

Pruebas de medición del ancho de banda

Para la medición del ancho de banda se realizaron dos pruebas con la herramienta IPERF a un ancho de banda de 10 Mbps y 20 Mbps. Ver figuras 4.22 y 4.23.

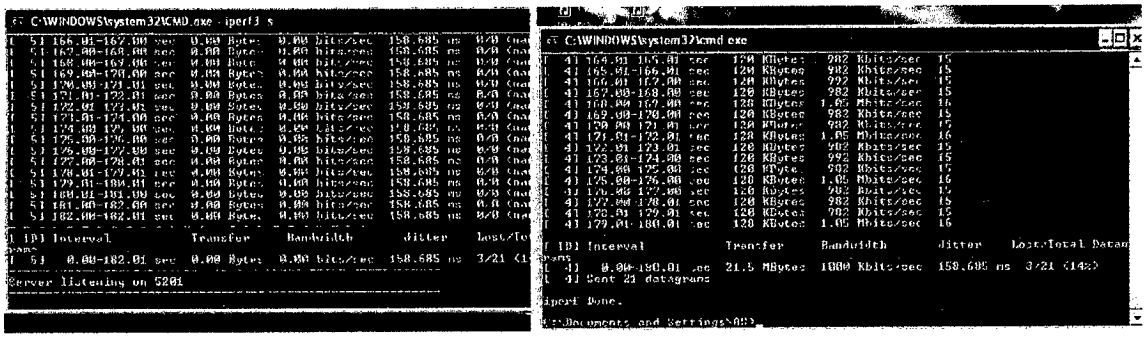


Figura 4.22 Ancho de banda a 10 Mbps en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

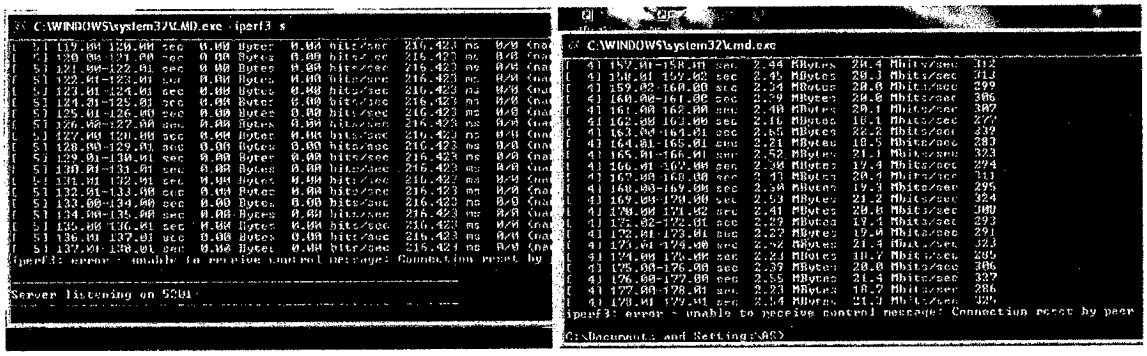


Figura 4.23 Ancho de banda a 20 bps en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

Las dos pruebas sobre la red (10 y 20 Mbps) arrojaron los resultados mostrados en la tabla 4.6.

Ancho de banda	Ancho de banda obtenido.	Jitter (ms)
10 Mbps	10.0	158.685
20 Mbps	19.8	216.423

Tabla 4.6 Resultados de pruebas del ancho de banda en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

Pruebas de medición del tiempo de convergencia

Para medir el tiempo de convergencia, se reinició dos veces la sesión BGP en el router PE2. En ese momento el sniffer conectado al router, que ya había iniciado la captura de tramas segundos antes, muestra las tramas BGP que anuncian las rutas. Ahora aquí encontramos la sesión de los vecinos 23.23.23.2 a 23.23.23.3, es decir, del router PE2 al router PE3.

Luego de la ejecución del comando "clear ip bgp" en PE2 y realizada la prueba, el primer mensaje BGP OPEN de la sesión PE2 a PE3 llega a los 102.703 segundos de iniciada la captura y anuncia el número 23.23.23.2 que identifica al router PE2. La figura 4.24 muestra dicha trama.

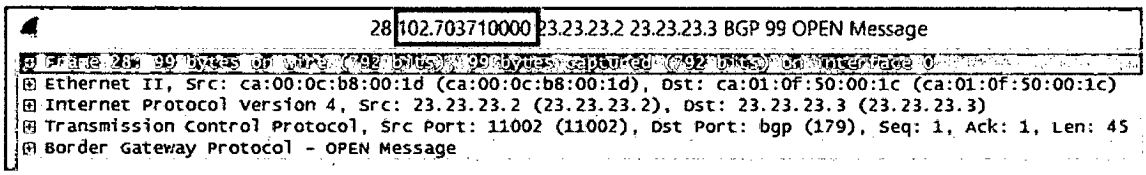


Figura 4.24 Primer mensaje BGP OPEN en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

De igual forma, para la sesión PE2 a PE2 a PE3 el último mensaje BGP UPDATE llega a los 102.9217 segundos de iniciada la captura.

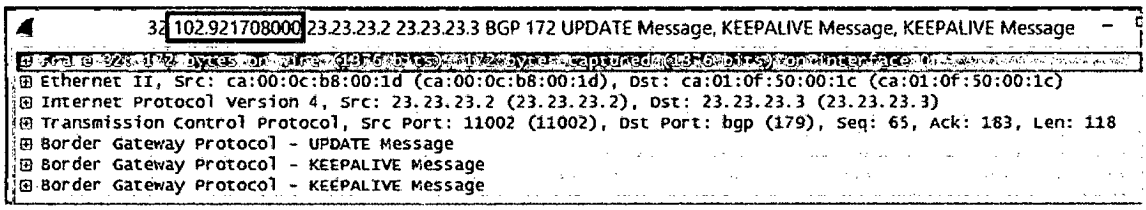


Figura 4.25 Ultimo mensaje BGP UPDATE en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

En la tabla 4.7, se muestran los resultados del tiempo de convergencia.

Mensaje BGP	Tiempo de llegada (s)
Open BGP	102.703
Update BGP	102.9217
Tiempo de Convergencia	0.218

Tabla 4.7 Resultados de pruebas del tiempo de convergencia en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

Lo cual tenemos una variación de tiempo de 0.218 segundos.

Pruebas del uso del CPU

Para la prueba de utilización del CPU del router, se reinició la sesión BGP en los routers de borde, es decir, primero con PE2. Aquí utilizaremos el comando *show processes cpu history* en los vecinos de los routers mencionados. En las siguientes imágenes se muestran los resultados obtenidos

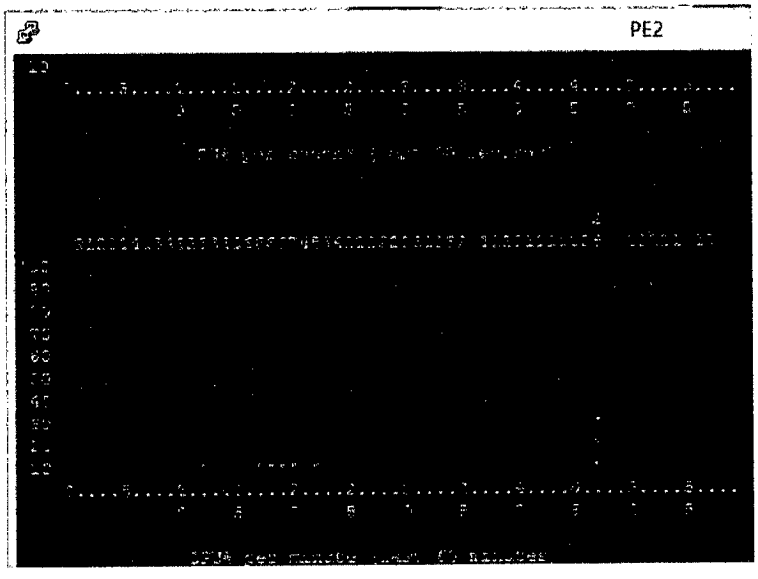


Figura 4.26 Uso del CPU con reinicio BGP en router PE2 en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

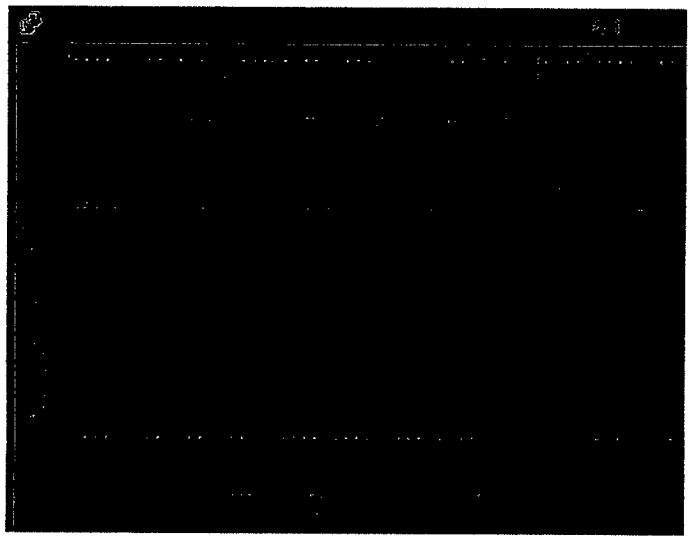


Figura 4.27 Uso del CPU con reinicio BGP en router PE3 en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

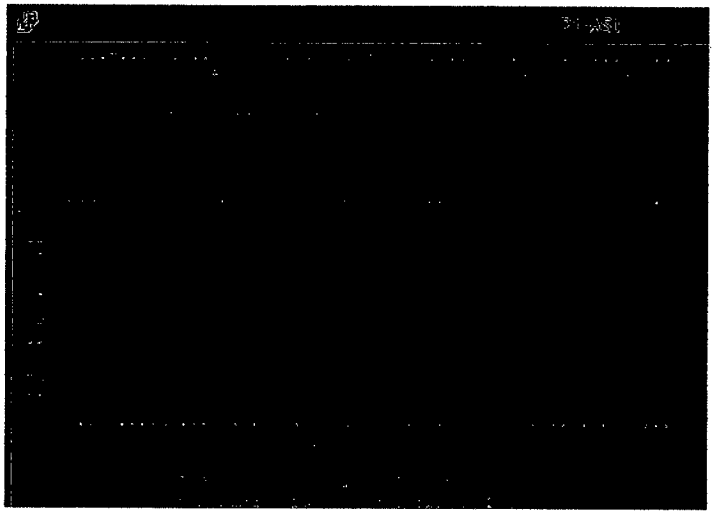


Figura 4.28 Uso del CPU con reinicio BGP en router P1-AS1 en el modelo Modelo 2 - Next-hop-self (Elaboración Propia)

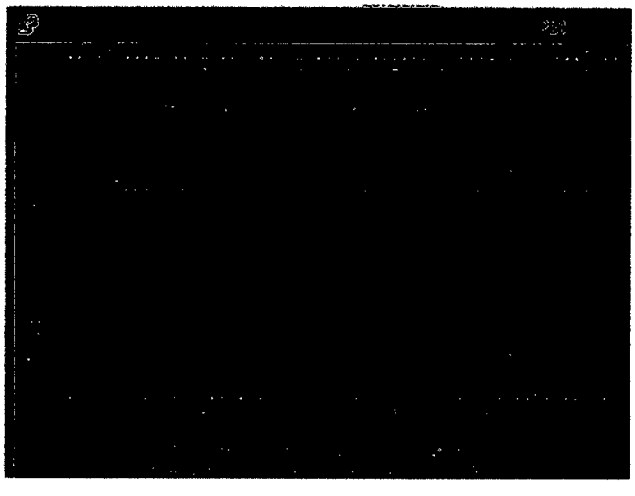


Figura 4.29 Uso del CPU con reinicio BGP en router PE1 en el modelo modelo 2 - Next-hop-self (Elaboración Propia)

En la tabla 4.8, se muestran los resultados del uso del CPU

Equipo	Valor máximo del uso del CPU
Router PE2	5 %
Router PE3	22 %
Router P1-AS1	2 %
Router PE1	13%

Tabla 4.8 Resultados del uso del CPU en el modelo 2 - Next-hop-self (Elaboración Propia)

Análisis de la implantación del Modelo 2 - MP-eBGP entre ASBRs - Next-hop-self

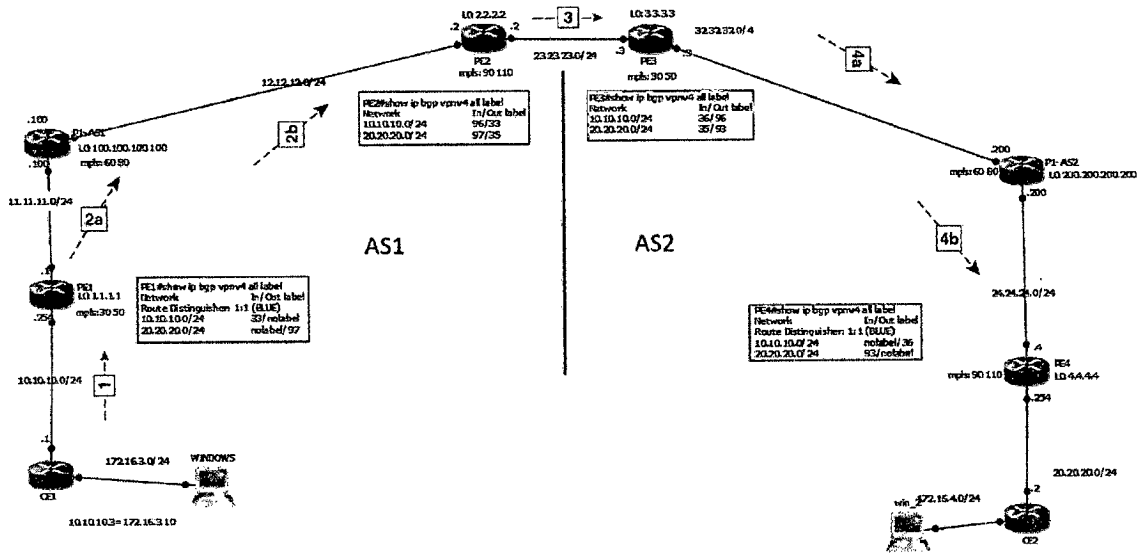


Figura 4.30 Implementación Modelo 2 - Next-hop-self (Elaboración Propia)

De la figura 4.30 se tiene que:

1. El router CE1 envía la red 10.10.10.0/24 como una actualización IPV4 al router PE1.

2A. Como parte de la operación LDP/LDP, PE1 envía un "implicit-null" o "POP label" (11.11.11.2) que es el "next hop" (siguiente salto) en la actualización VPNv4 10.10.10.0/24. Esto es indicado para el router P1-AS1 a la etiqueta "pop label" en el reenvío del paquete de datos desde CE2 a CE1.

2B. El router P1-AS1 genera una etiqueta LDP 60 para el siguiente salto en la actualización 10.10.10.0/24.

3. El router PE2 cambia el siguiente salto por si mismo cuando se esta propagando la ruta exterior en su propio sistema autonomo. PE2 además localiza una nueva etiqueta 96 y envía la ruta VPNv4 al router PE3.

4A. Como parte de la operación LDP/LDP, PE1 envía un "POP label" a PE3, que es el siguiente salto de la actualización VPNv4 10.10.10.0/24. Esto es indicado para el router P1-AS1 al "pop" de la etiqueta LDP en el reenvío del paquete de datos en la actualización 10.10.10.0/24.

4B. El router P1-AS2 genera una etiqueta 61 para el siguiente salto que es el router PE2 en la actualización VPNv4 10.10.10.0/24

1. El router PE2 tiene configurado el VRF BLUE para aceptar rutas con RT 1:1 y además traducir las actualizaciones VPNv4 a IPv4 e insertar la ruta en VRF BLUE. Esto propaga esta ruta a CE2. En la siguiente figura tenemos la distribución de etiquetas y después el respectivo tracer del router CE1 a PC2 y el router CE2 a PC1.

En la figura 4.32 tenemos la distribución de etiquetas y después el respectivo tracer del router CE1 a PC2 y el router CE2 a PC1.

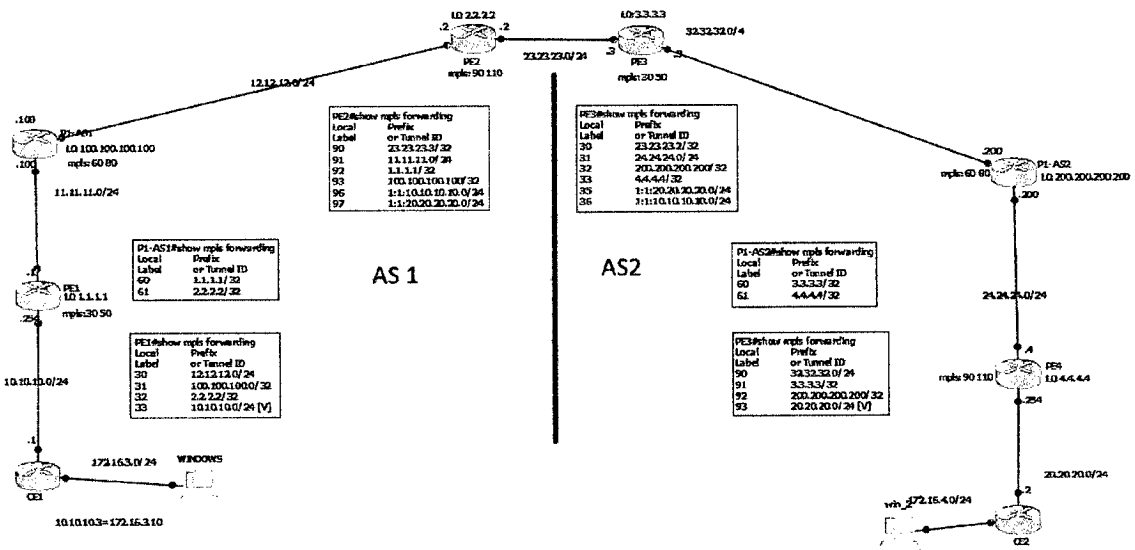


Figura 4.31 Distribución de etiquetas en la implementación del modelo 2 - Next-hop-self (Elaboración Propia)

```
CE1(config)#do tracer 20.20.20.3

Type escape sequence to abort.
Tracing the route to 20.20.20.3

  1 10.10.10.254 40 msec 32 msec 28 msec
  2 11.11.11.100 [MPLS: Labels 61/97 Exp 0] 92 msec 112 msec 80 msec
  3 12.12.12.2 [MPLS: Label 97 Exp 0] 112 msec 100 msec 128 msec
  4 23.23.23.3 [MPLS: Label 35 Exp 0] 120 msec 116 msec 80 msec
  5 32.32.32.200 [MPLS: Labels 61/95 Exp 0] 132 msec 136 msec 104 msec
  6 20.20.20.254 96 msec 76 msec 64 msec
  7 20.20.20.2 152 msec 136 msec 156 msec
```

Figura 4.32 Tracert exitoso entre el router CE1 al PC2 en el modelo 2 - Next-hop-self (Elaboración Propia)

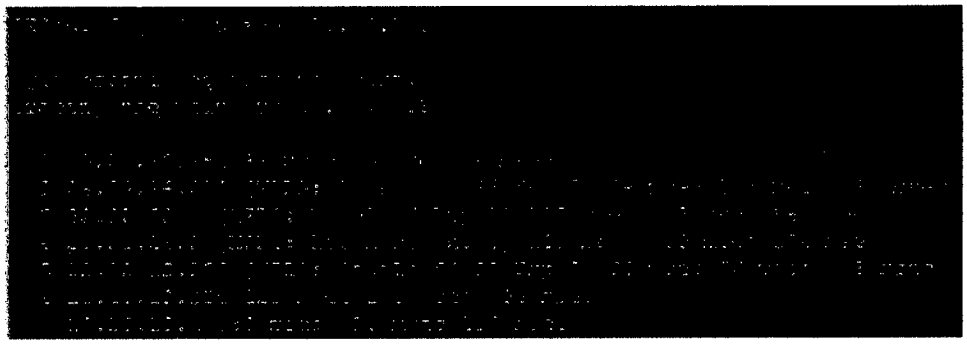


Figura 4.33 Tracert exitoso entre el router CE2 al PC1 en el modelo 2 - Next-hop-self (Elaboración Propia)

4.1.2.3 Modelo 3: MP-eBGP entre ASBRs - Redistribute connected

En la topología que se muestra en la figura 4.34 se ha considerado al igual que en el caso anterior un total de 8 routers y dos hosts, uno de origen y el otro de destino, ambos ubicados en los extremos de la red. En este modelo cada ABSR (PE2 y PE3) acepta la ruta sin cambiar el siguiente salto ni la etiqueta, que continúan siendo los del ASBR remoto. Lo que se hace en su lugar es redistribuir las redes directamente conectadas dentro del IGP para anunciar el siguiente salto de las rutas recibidas desde el ASBR remoto.

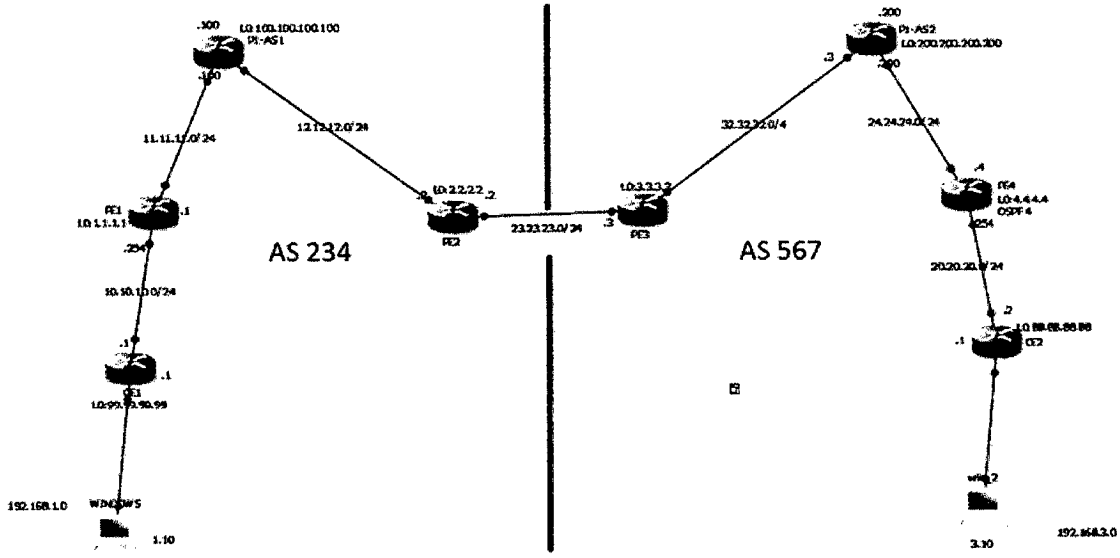


Figura 4.34 Topología de simulación del modelo 3 - MP-eBGP entre ASBRs - Redistribute connected (Elaboración Propia)

Éstos routers receptores crean una ruta para un host /32 para su vecino ASBR para acceder a la dirección del prefijo del siguiente salto. La ruta del host debe ser redistribuida dentro de IGP usando el comando "redistribute connected".

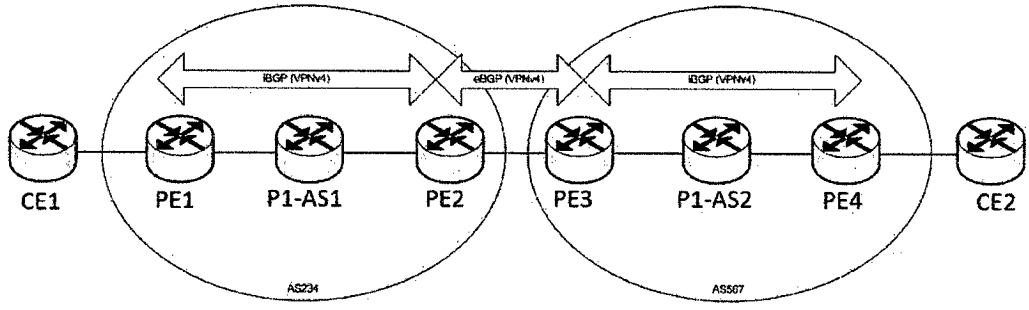


Figura 4.35 Esquema del modelo 3 - MP-eBGP entre ASBRs - Redistribute connected (Elaboración Propia)

Pruebas de conexión extremo-extremo

La validación de la conectividad conectividad entre los equipos finales del cliente, es similar que en los dos modelos anteriores, se realizó la acción ping con un número de repeticiones de 200 y 500 desde la PC1 a PC2 y en simultáneo desde PC2 a PC1.

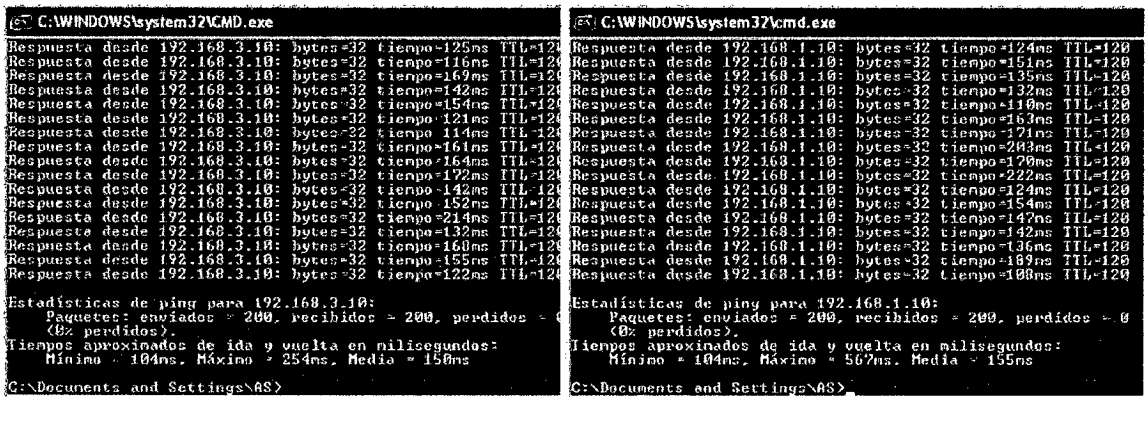


Figura 4.36 Ping con 200 repeticiones en el modelo 3 - Redistribute connected (Elaboración Propia)

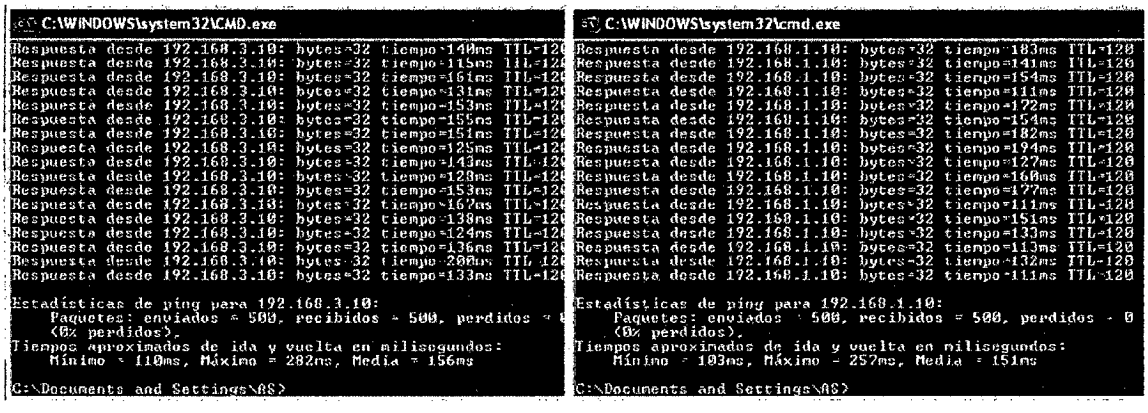


Figura 4.37 Ping con 500 repeticiones en el modelo 3 - Redistribute connected (Elaboración Propia)

Número de repeticiones	Retardo promedio de PC1 A PC2	Retardo promedio de PC2 A PC1
200	150 ms	155 ms
500	156 ms	151 ms

Tabla 4.9 Resultados de la conectividad entre las sedes del cliente en el modelo 3 - Redistribute connected (Elaboración Propia)

Pruebas de medición del ancho de banda

Al igual que en los modelos anteriores, para la medición del ancho de banda se realizaron tres pruebas con la herramienta IPERF a un ancho de banda de 10 Mbps y 20 Mbps.

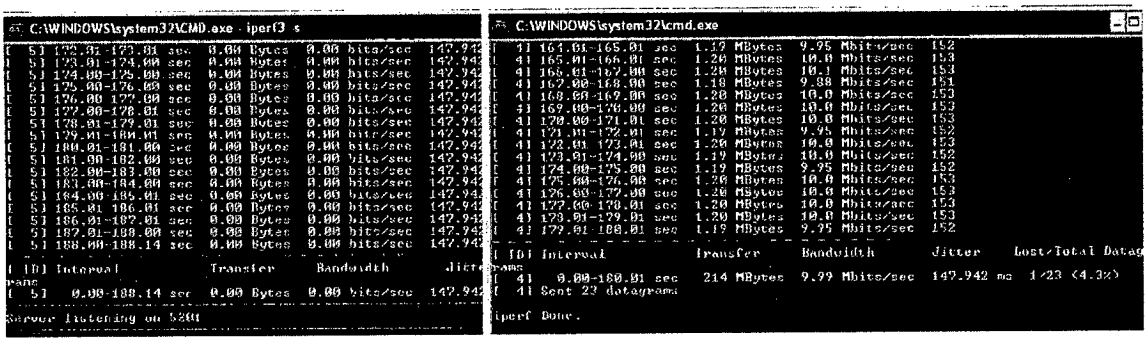


Figura 4.38 Ancho de banda a 10 Mbps en el modelo 3 - Redistribute connected (Elaboración Propia)

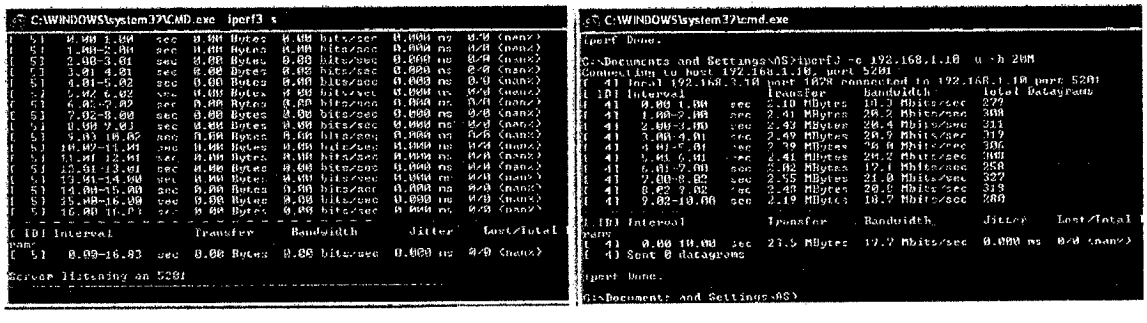


Figura 4.39 Ancho de banda a 20 Mbps en el modelo 3 - Redistribute connected (Elaboración Propia)

La tabla 4.10 muestra los resultados de las tres pruebas.

Ancho de banda (Mbps)	Ancho de banda obtenido (Mbps)	Jitter (ms)
10 Mbps	9.99	147.942
20 Mbps	19.7	0.0

Tabla 4.10 Resultados de pruebas del ancho de banda en el modelo 3 - Redistribute connected (Elaboración Propia)

Pruebas de medición del tiempo de convergencia

La medición del tiempo de convergencia es similar en todos los casos, se reinició dos veces la sesión BGP en el router PE2. En ese momento el sniffer conectado al router, que ya había iniciado la captura de tramas segundos antes, muestra las tramas BGP que anuncian las rutas. Ahora aquí encontramos la sesión de los vecinos 23.23.23.2 a 23.23.23.3, es decir, del router PE2 al router PE3.

Luego de la ejecución del comando "clear ip bgp" en PE2 y realizada la prueba, el primer mensaje BGP OPEN de la sesión PE2 a PE3 llega a los 124.3890 segundos de iniciada la captura y anuncia el número 23.23.23.2 que identifica al router PE2. La figura 4.40 muestra dicha trama.

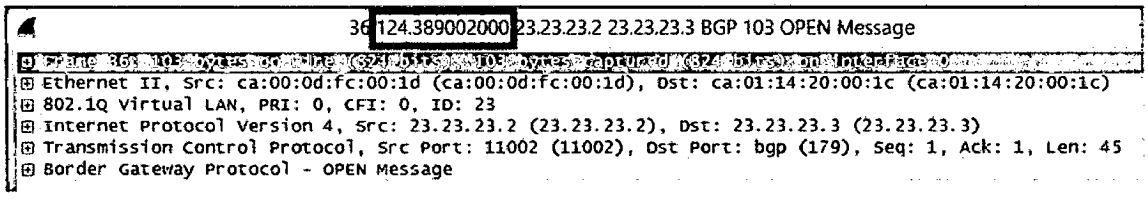


Figura 4.40 Primer mensaje BGP OPEN en el modelo 3 - Redistribute connected (Elaboración Propia)

De igual forma, para la sesión PE2 a PE3 el último mensaje BGP UPDATE llega a los 99.661 segundos de iniciada la captura, vemos que el router PE2 entrega el mensaje update con una etiqueta 60 que es la etiqueta asignado por el router P1-AS1 tal como se muestra en la figura 4.41.

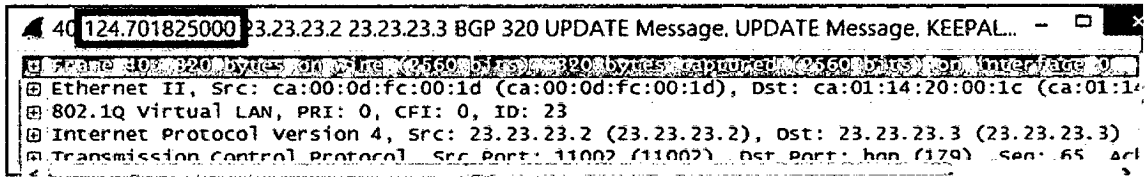


Figura 4.41 Ultimo mensaje BGP UPDATE en el modelo 3 - Redistribute connected (Elaboración Propia)

En la tabla 4.11, se muestran los resultados del tiempo de convergencia

Mensaje BGP	Tiempo de llegada (s)
Open BGP	124.389
Update BGP	124.701
Tiempo de Convergencia	0.312

Tabla 4.11 Resultados de pruebas del tiempo de convergencia en el modelo 3 - Redistribute connected (Elaboración Propia)

Lo cual tenemos una variación de tiempo de 0.312 segundos.

Pruebas del uso del CPU

Para la prueba de utilización del CPU del router, se reinició la sesión BGP en los routers de borde, es decir, primero con PE2. Aquí utilizaremos el comando *show processes cpu history* en los vecinos de los routers mencionados. En las siguientes imágenes se muestran los resultados obtenidos

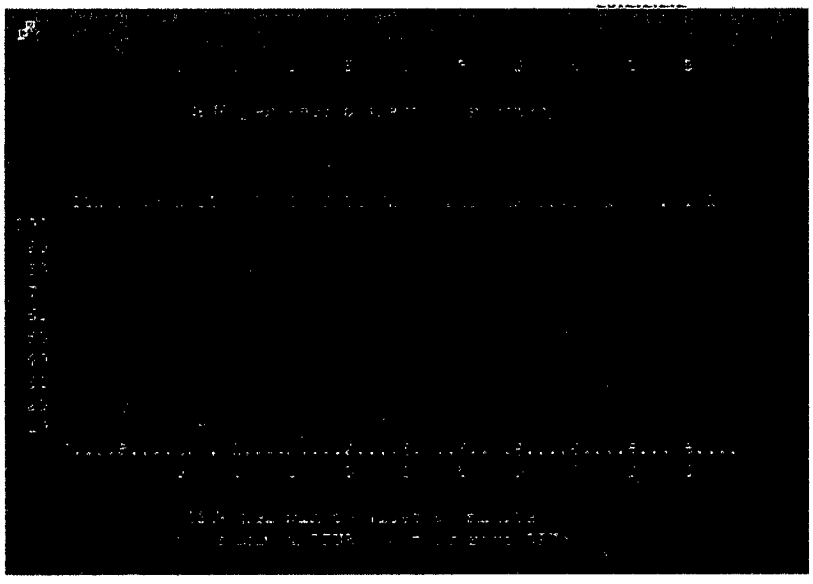


Figura 4.42 Uso del CPU con reinicio BGP en router PE2 en el modelo 3 - Redistribute connected (Elaboración Propia)

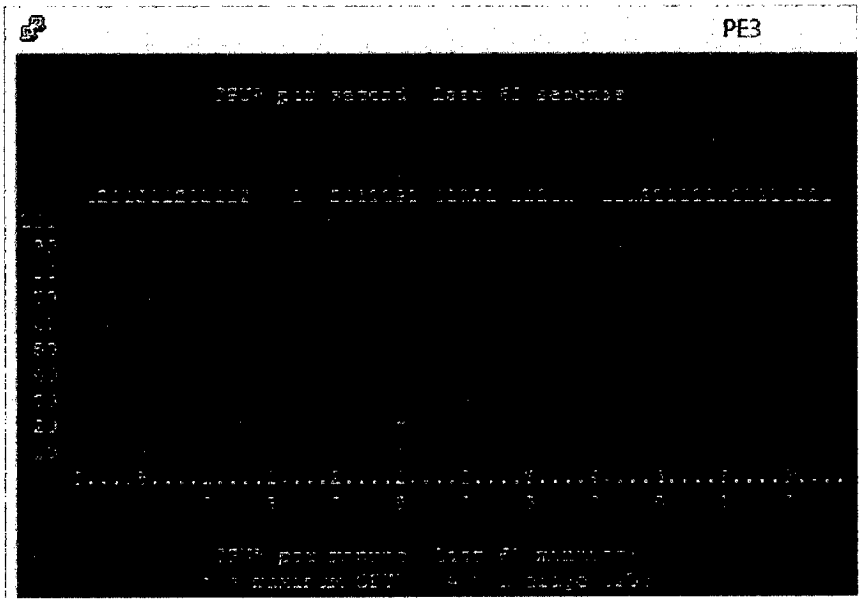


Figura 4.43 Uso del CPU con reinicio BGP en router PE3 en el modelo 3 - Redistribute connected (Elaboración Propia)

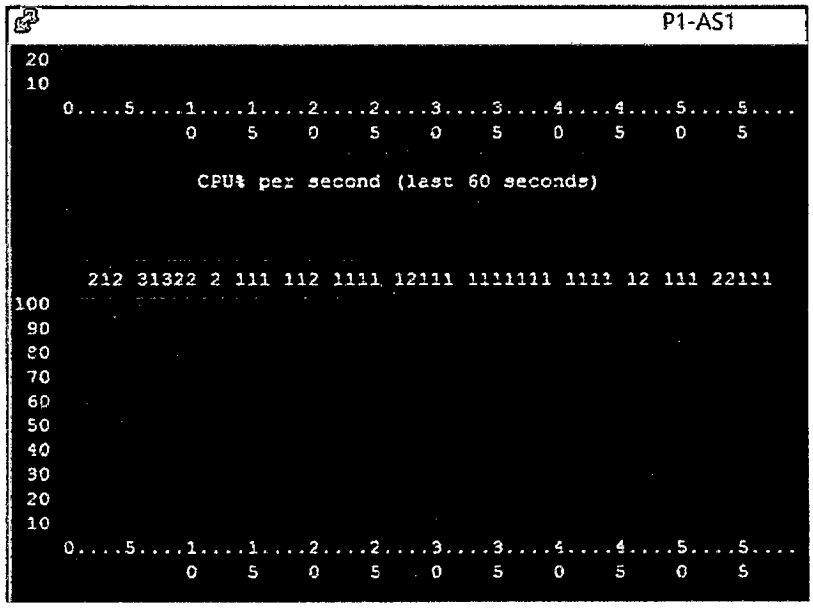


Figura 4.44 Uso del CPU con reinicio BGP en router P1-AS1 en el modelo 3 - Redistribute connected (Elaboración Propia)

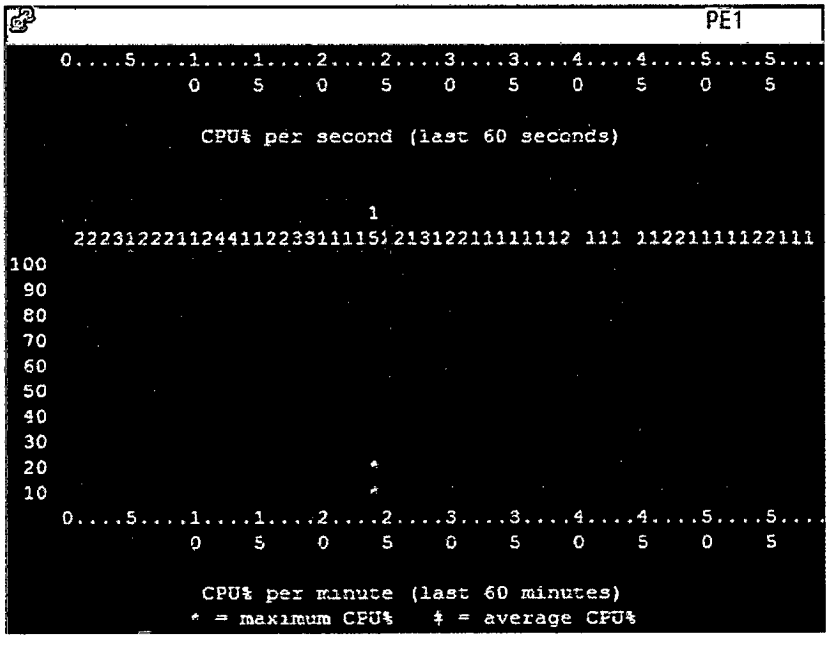


Figura 4.45 Uso del CPU con reinicio BGP en router PE1 en el modelo 3 - Redistribute connected (Elaboración Propia)

En la tabla 4.12, se muestran los resultados del uso del CPU

Equipo	Valor máximo del uso del CPU
Router PE2	4 %
Router PE3	19 %
Router P1-AS1	2 %
Router PE1	15%

Tabla 4.12 Resultados del uso del CPU en el modelo 3 - Redistribute connected (Elaboración Propia)

Análisis de la implantación del modelo 3 MP-eBGP entre ASBRs - Redistribute connected

La figura 4.46 muestra la acción del plano del control de reenvío que toma lugar la advertencia del prefijo 10.10.10.0/24 por CE1 a CE2 que pertence a la VRF R1 y R2

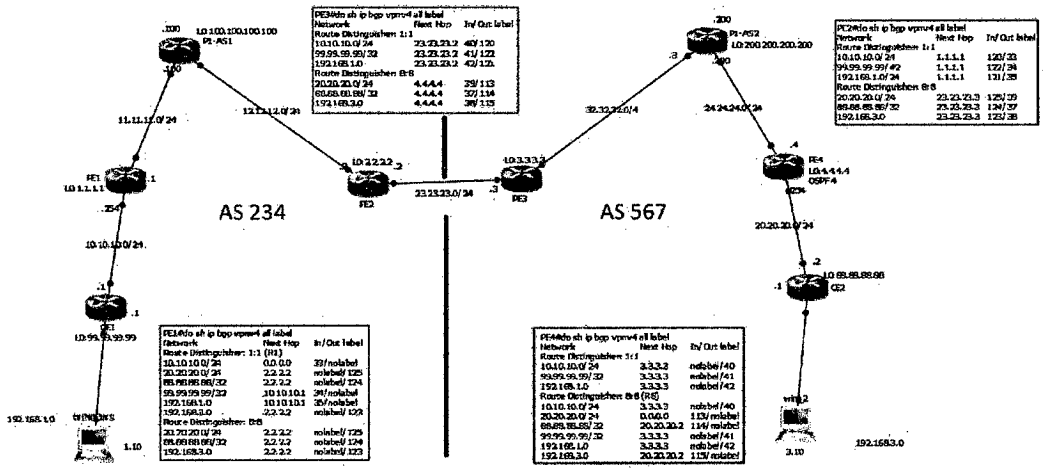


Figura 4.46 Implementación modelo 3- MP-eBGP entre ASBRs - Redistribute connected

En la figura 4.47 tenemos la distribución de etiquetas y después el respectivo tracer del router CE1 a PC2 y el router CE2 a PC1.

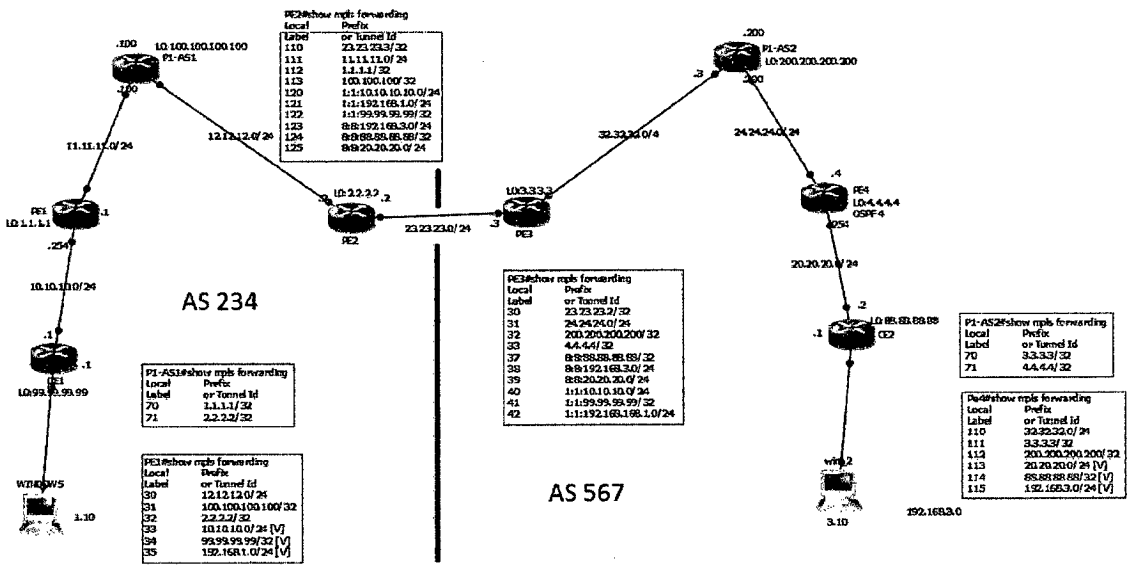


Figura 4.47 Distribución de etiquetas en la implementación del modelo 3 - Redistribute connected (Elaboración Propia)

Figura 4.48 Tracert exitoso entre el router CE1 al PC2 en el modelo 3 - Redistribute connected (Elaboración Propia)

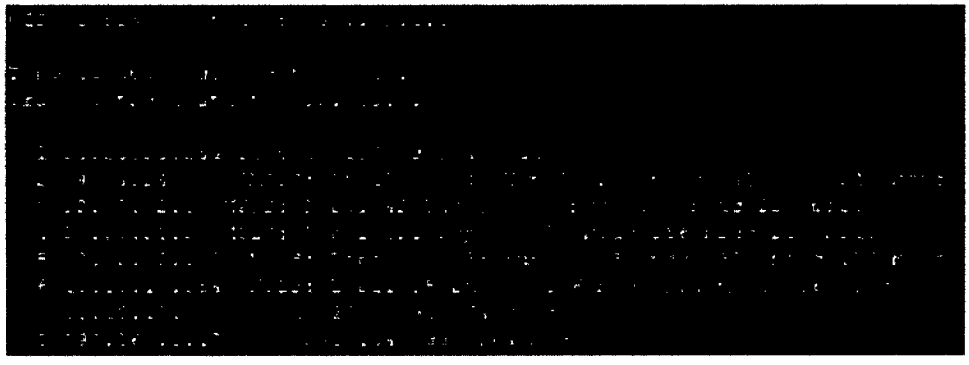


Figura 4.49 Tracert exitoso entre el router CE2 al PC1 en el modelo 3 - Redistribute connected (Elaboración Propia)

4.1.2.4 Modelo 4: Multihop MP-eBGP entre Route-Reflectors (RRs)

El modelo MPLS VPN - Route Target Rewrite tiene la característica de sustituir los "router target" entrantes y reemplazarlos con actualizaciones salientes de BGP. Típicamente, los router ASBR realiza la sustitución de los "router target" en los bordes de los sistemas autónomos. Los router reflectores y los del cliente pueden realizar los "route target"

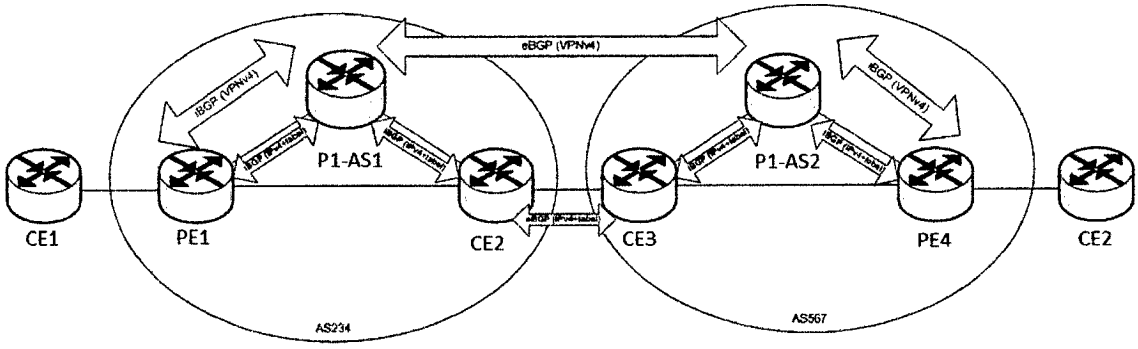


Figura 4.50 Esquema del modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

La principal ventaja de este modelo es que mantiene la administración de la política local en el sistema autónomo de enrutamiento.

En la topología que se muestra en la figura 4.51 los routers P1-AS1 y P1-AS serán los Route Reflectors y en donde se establecerá la sesión MP-eBGP.

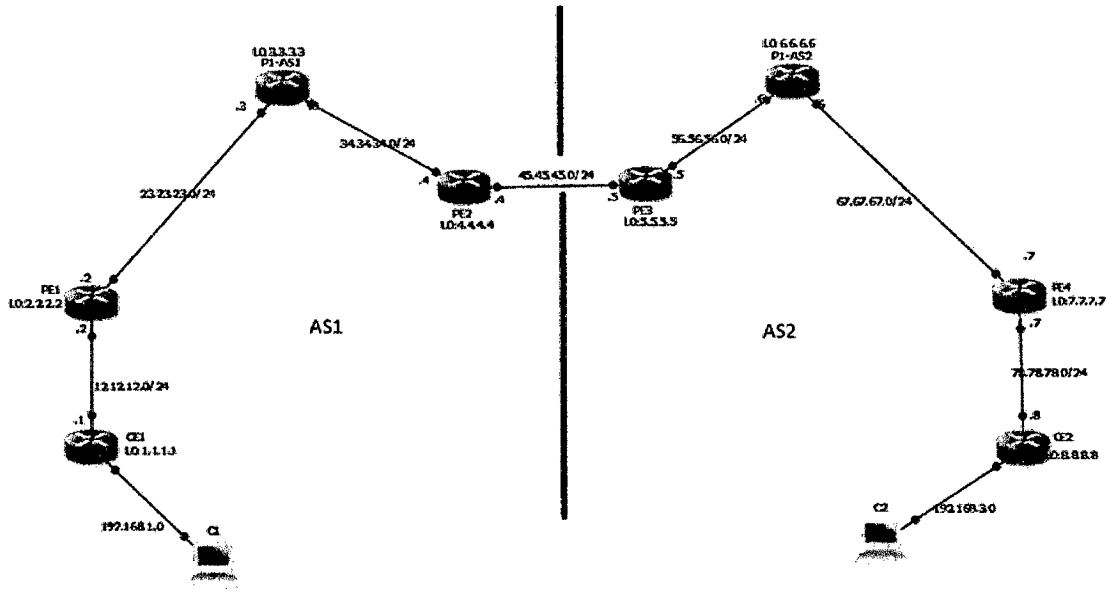


Figura 4.51 Topología de simulación del modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Pruebas de conexión extremo-extremo

Para verificar la conectividad entre los equipos finales del cliente se realizó la acción ping con un número de repeticiones de 200 y 500 desde la PC1 a PC2 y en simultáneo desde PC2 a PC1, ver figura 4.52 con 200 repeticiones y figura 4.53 con 500 repeticiones.

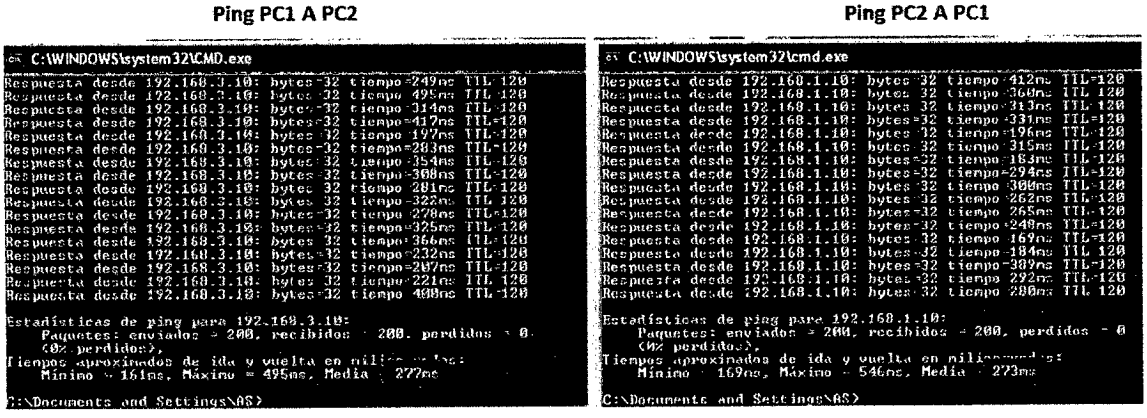


Figura 4.52 Ping con 200 repeticiones en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

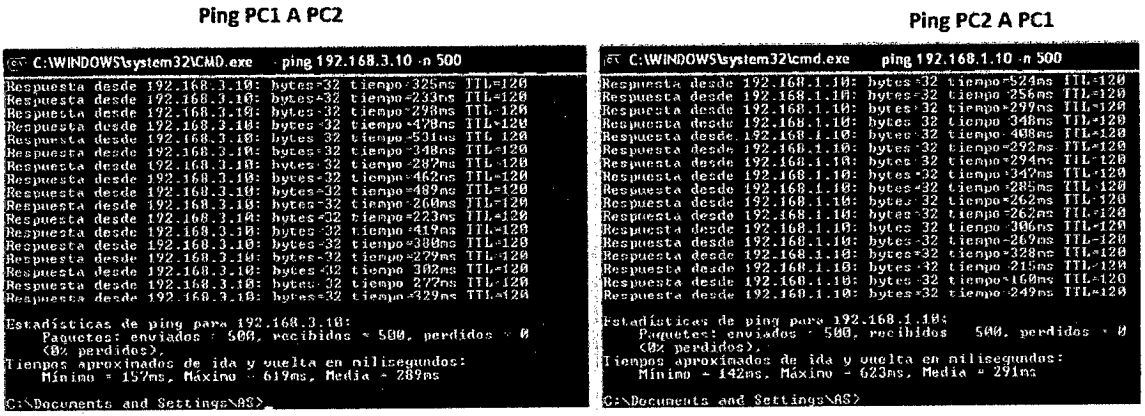


Figura 4.53 Ping con 500 repeticiones en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Las pruebas de conexión fue un éxito y se logró conectividad entre los equipos finales del cliente. Los resultados de estas pruebas se muestran en la tabla 4.13.

Número de repeticiones	Retardo promedio de PC1 A PC2	Retardo promedio de PC1 A PC2
200	277 ms	273 ms
500	289 ms	291 ms

Tabla 4.13 Resultados de la conectividad entre las sedes del cliente en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Pruebas de medición del ancho de banda

Para la medición del ancho de banda se realizaron dos pruebas con la herramienta IPERF a un ancho de banda de 10 Mbps y 20 Mbps.

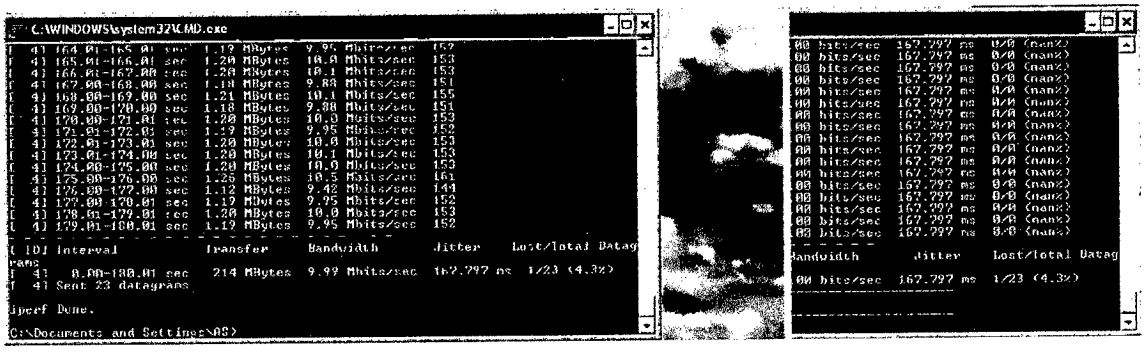


Figura 4.54 Ancho de banda a 10 Mbps en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

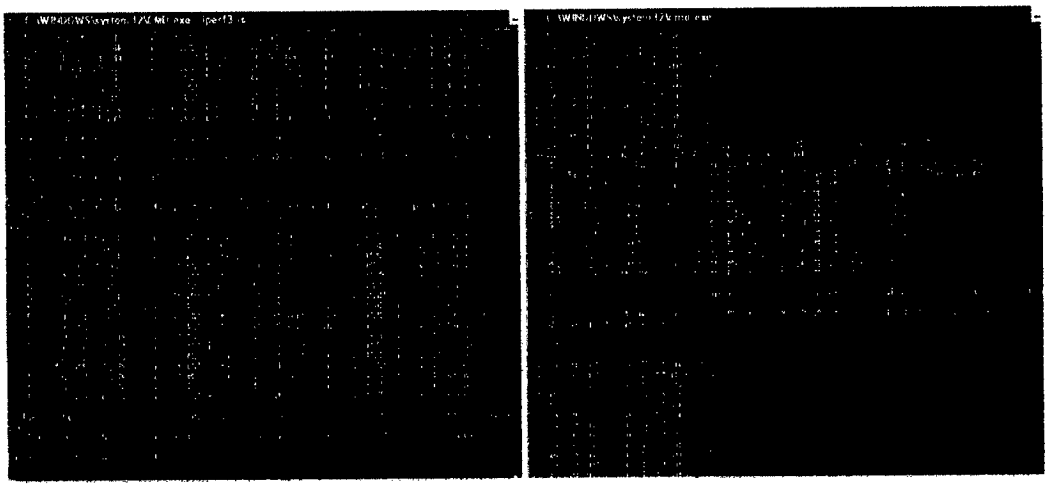


Figura 4.55 Ancho de banda a 20 Mbps en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Las dos pruebas sobre la red (10 y 20 Mbps) arrojaron los resultados mostrados en la tabla 4.14.

Ancho de banda (Mbps)	Ancho de banda obtenido (Mbps)	Jitter (ms)
10 Mbps	9.90	167.797
20 Mbps	19.8	212.301

Tabla 4.14 Resultados de pruebas del ancho de banda en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Pruebas de medición del tiempo de convergencia

Para medir el tiempo de convergencia, se reinició dos veces la sesión BGP en el router PE2. En ese momento el sniffer conectado al router, que ya había iniciado la captura de tramas segundos antes, muestra las tramas BGP que anuncian las rutas. Ahora aquí encontramos la sesión de los vecinos 45.45.45.4 a 45.45.45.5, es decir, del router PE2 al router PE3.

En el primer reinicio, el primer mensaje BGP OPEN de la sesión PE2 a PE3 llega a los 41.883 segundos de iniciada la captura y anuncia el número 45.45.45.4 que identifica al router PE2. La figura 4.56 muestra dicha trama.

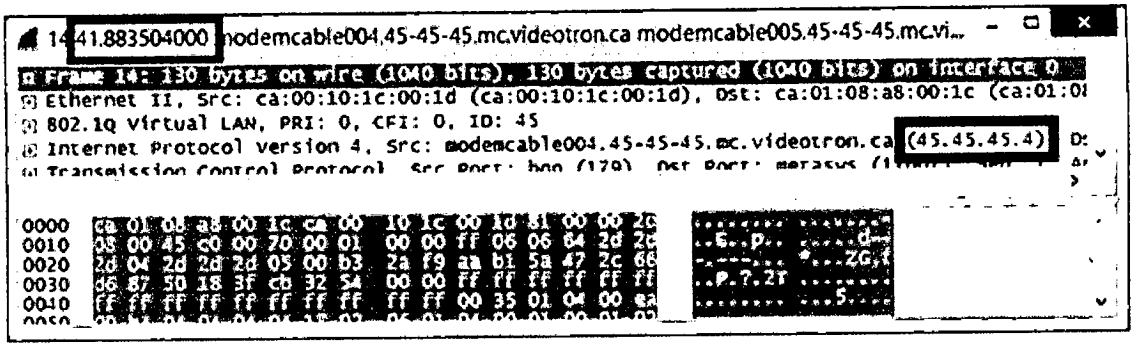


Figura 4.56 Primer mensaje BGP OPEN en el primer reincio BGP en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

De igual forma, para la sesión PE2 a PE3 el último mensaje BGP UPDATE llega a los 42.305 segundos de iniciada la captura, la cual es mostrada en la figura 4.57.

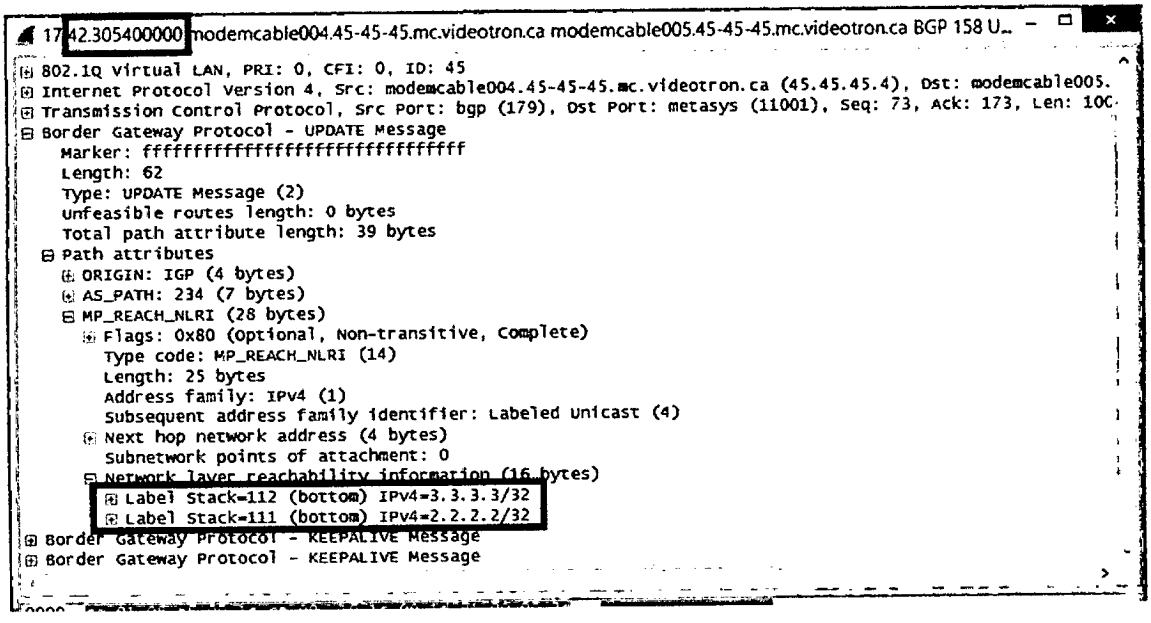


Figura 4.57 Ultimo mensaje BGP UPDATE en el primer reincio BGP en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

En el segundo reinicio, el primer mensaje BGP OPEN de la sesión PE2 a PE3 llega a los 57.510 segundos de iniciada la captura y anuncia el número 45.45.45.4 que identifica al router PE2. La figura 4.58 muestra dicha trama.

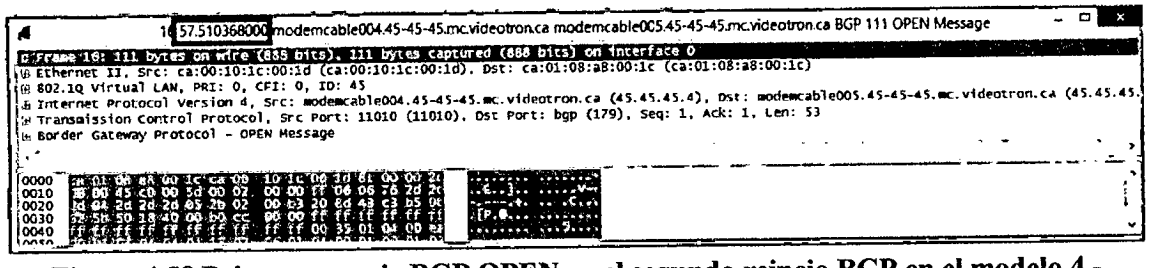


Figura 4.58 Primer mensaje BGP OPEN en el segundo reincio BGP en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

De igual forma, para la sesión PE2 a PE3 el último mensaje BGP UPDATE llega a los 57.869 segundos de iniciada la captura, la cual es mostrada en la figura 4.59.

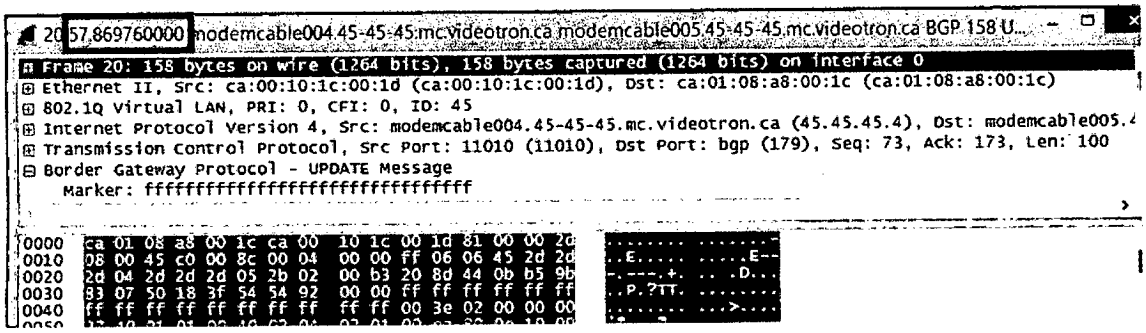


Figura 4.59 Ultimo mensaje BGP UPDATE en el segundo reincio BGP en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

En la tabla 4.15, se muestran los resultados del tiempo de convergencia.

Mensaje BGP	Tiempo de llegada en el primer reinicio (seg)	Tiempo de llegada en el segundo reinicio (seg)
Open BGP	41.883	57.510
Update BGP	42.305	57.869
Tiempo de convergencia	0.422	0.349

Tabla 4.15 Resultados de pruebas del tiempo de convergencia en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Lo cual tenemos un promedio de: $\frac{0.422+0.349}{2} = 0.3905\ seg$

Pruebas del uso del CPU

Para la prueba de utilización del CPU del router, se reinició la sesión BGP en los routers de borde, es decir, primero con PE2 y luego en PE3. Aquí utilizaremos el comando *show processes cpu history* en los vecinos de los routers mencionados. En las siguientes figuras se muestran los resultados obtenidos

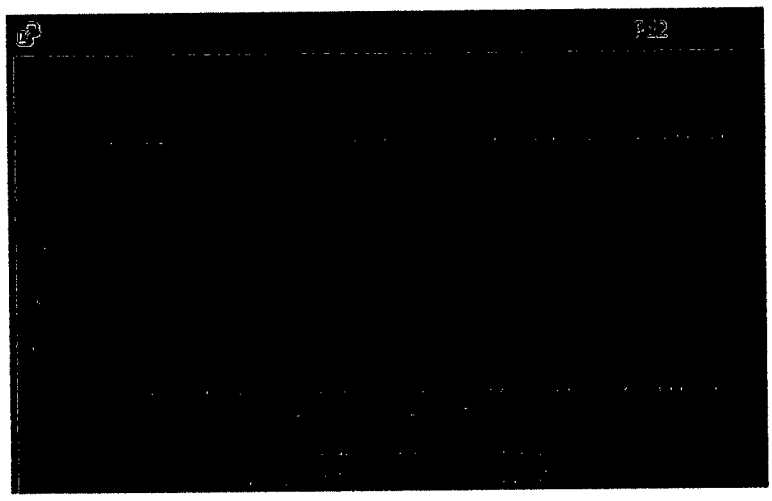


Figura 4.60 Uso del CPU con reinicio BGP en router PE2 en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

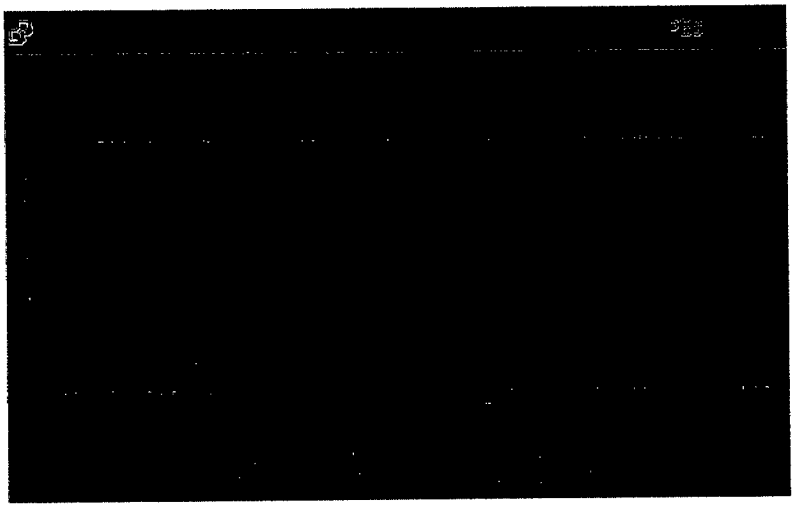


Figura 4.61 Uso del CPU con reinicio BGP en router PE3 en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

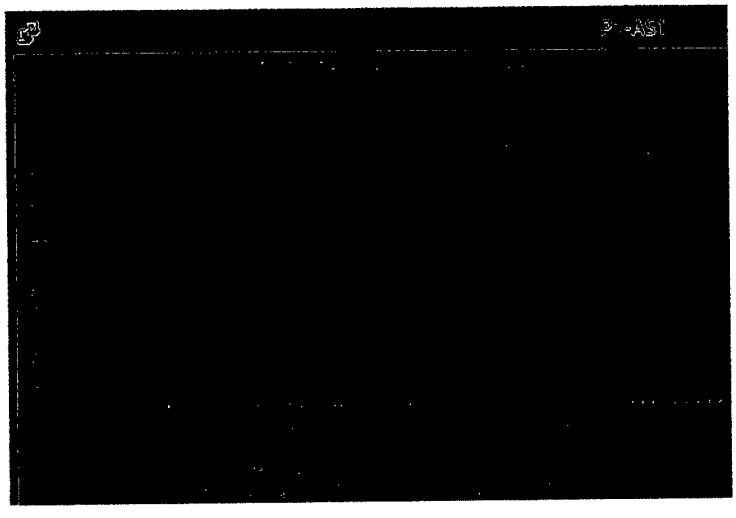


Figura 4.62 Uso del CPU con reinicio BGP en router P1-AS1 en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Donde observamos que para PE2 tiene una variación entre 3% y 4% - pese a que en este router se reinició el proceso BGP AS 234 – lo cual no varía mucho, ahora con PE3 tiene un pico máximo de 28% y para P1-AS1 con 10 %. En la tabla 4.16, se muestran los resultados del uso del CPU.

Equipo	Valor máximo del uso del CPU
Router PE2	4 %
Router PE3	28 %
Router P1-AS1	10 %

Tabla 4.16 Resultados del uso del CPU en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Análisis de la implantación del Modelo 4

Este enfoque es considerado para ser más escalable que las primeras opciones. En esta opción, la información VPNVv4 es mantenida por los RRs (Router Reflectors), que en la topología, tanto los routers P1-AS1 y P1-AS2 realizan esta función.

Para reunir este requerimiento, cada proveedor necesita tener los RRs para la distribución de los prefijos VPNv4 e intercambiar los prefijos eBGP con las adyacencias externas. Los routers de borde en esta opción participan en el intercambio de next-hop-address BGP usando etiquetas IPv4, y los RRs transportan la información VPNv4.

La figura 4.63 muestra la operación de reenvio de los prefijos a través de cada router tanto en AS1 y AS2.

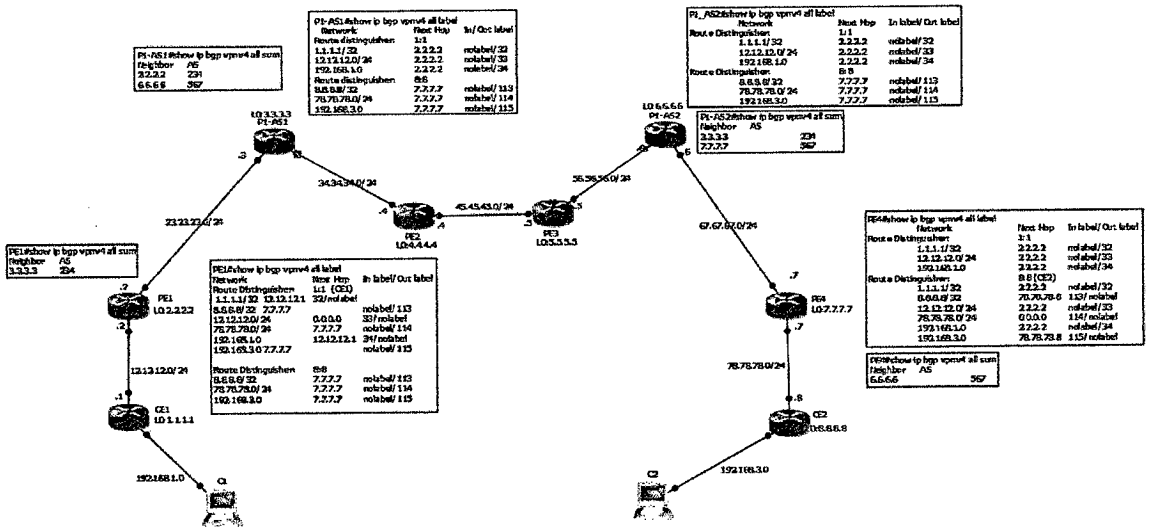


Figura 4.63 Implementación modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Como se menciono, P1-AS1 y P1-AS2 son los RRs, que son local en cada proveedor de servicios. Una sesión MP-eBGP esta formada entre los RRs para transportar información VPNv4 a través de ambos sistemas autónomos. Una sesión BGP está formada entre los ASBRs (routers de borde) para intercambiar los prefijos next-hop-address.

En la figura 4.64, por ejemplo, el router PE1 asigna etiquetas localmente (Local Label), es decir, rutas que no estén conectadas directamente, es por eso que la red 23.23.23.0/24 no se le asigna una etiqueta específica.

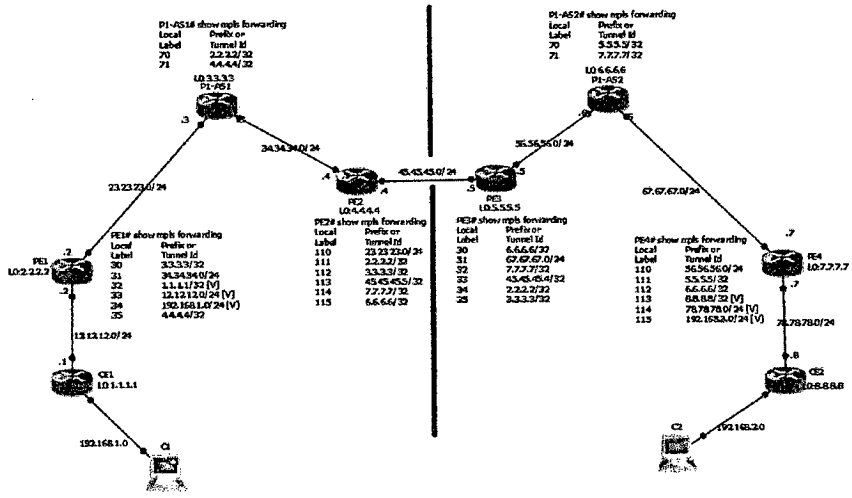


Figura 4.64 Distribución de etiquetas en la implementación del 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

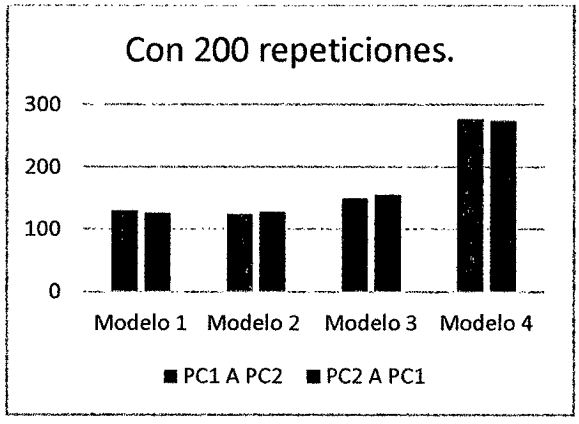
4.1.3 Comparación de datos

4.1.3.1 Comparación entre diferentes echo.

- Comparación de los modelos con un ping con echo = 200.

n = 200	PC1 A PC2	PC2 A PC1
Modelo 1	130	126
Modelo 2	124	128
Modelo 3	150	155
Modelo 4	277	273

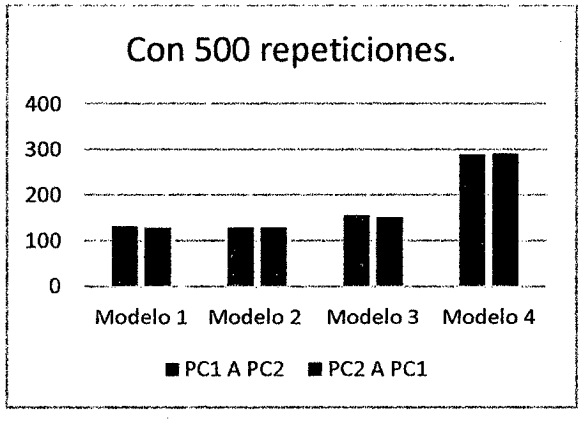
Tabla 4.17 Comparación de modelos de un ping con 200 repeticiones. (Elaboración Propia)



- Comparación de los modelos con un ping con echo = 500

n = 500	PC1 A PC2	PC2 A PC1
Modelo 1	131 ms	128 ms
Modelo 2	129 ms	129 ms
Modelo 3	156 ms	151 ms
Modelo 4	289 ms	291 ms

Tabla 4.18 Comparación de los modelos con un ping con 500 repeticiones. (Elaboración Propia)

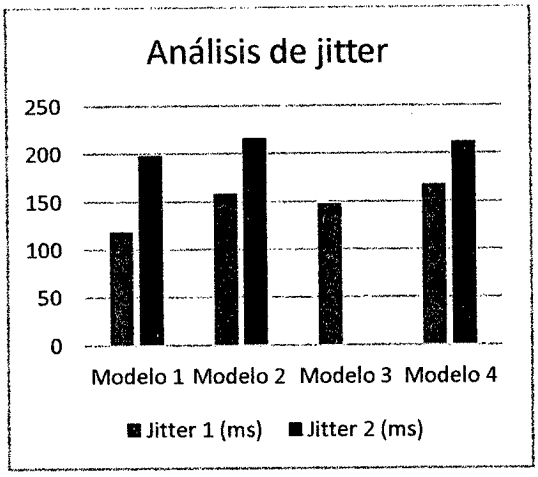


4.1.3.2 Comparación de cada modelo con herramienta IPERF

- Análisis de jitter:

Modelo	Jitter 1 (ms)	Jitter 2 (ms)
Modelo 1	119.064	198.553
Modelo 2	158.685	216.423
Modelo 3	147.942	0
Modelo 4	167.797	212.301

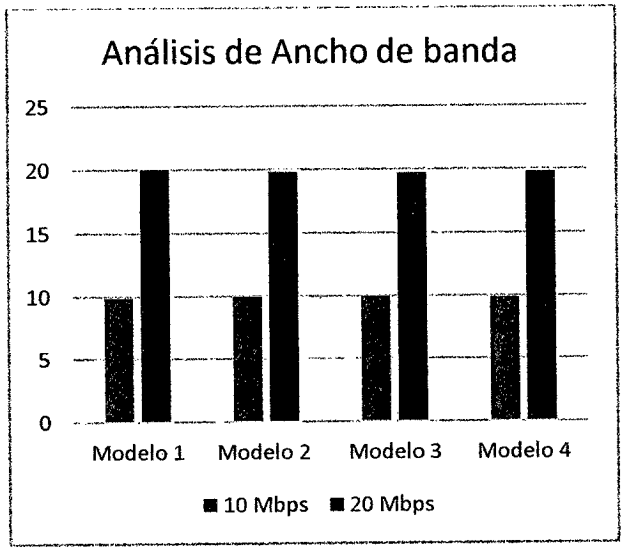
Tabla 4.19 Comparación de los modelos con herramienta Jitter, donde Jitter 1 es para un ancho de banda de 10 Mb/seg y Jitter 2 es para un ancho de banda de 20 Mb/seg. (Elaboración Propia)



- Comparación de medición

Modelo	10 Mbps	20 Mbps
Modelo 1	9.91	20
Modelo 2	10	19.8
Modelo 3	9.99	19.7
Modelo 4	9.9	19.8

Tabla 4.20 Comparación de ancho de banda obtenido. (Elaboración Propia)



4.1.3.3 Análisis de tiempo de convergencia.

Modelo	Tiempo de convergencia.(ms)
Modelo 1	33.719
Modelo 2	0.218
Modelo 3	0.312
Modelo 4	0.3905

Tabla 4.21 Comparación de los tiempos de convergencia de cada modelo. (Elaboración Propia)

4.1.3.4 Comparación del comando "show proc cpu history" después de reseteo de proceso BGP.

Modelo	PE2	PE3	PE1	P1-AS1
Modelo 1	10%	2%	9%	1%
Modelo 2	5%	22%	13%	2%
Modelo 3	4%	19%	15%	2%
Modelo 4	4%	28%		

Tabla 4.22 Comparación del uso del cpu del router. (Elaboración Propia)

4.1.3.5 Comparación del retardo del streaming para cada modelo.

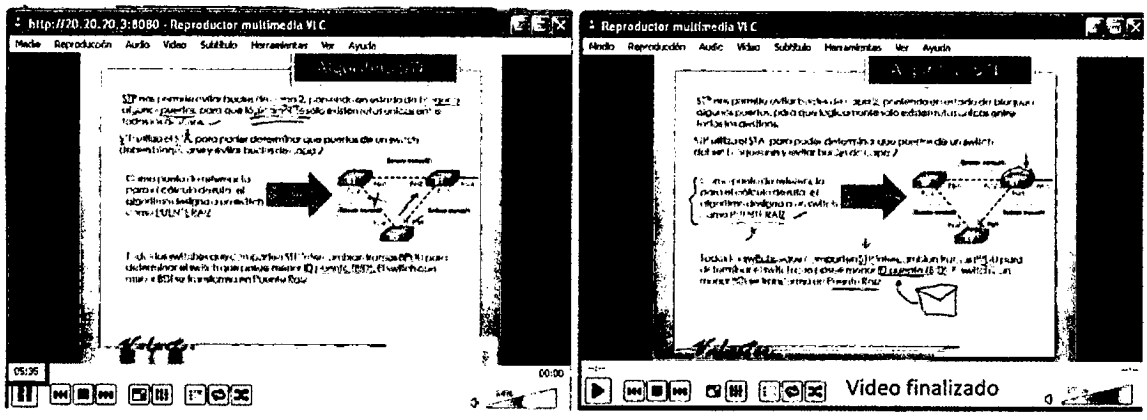


Figura 4.65 Retardo del streaming en el modelo 1 - Back-to-Back VRFs (Elaboración Propia)

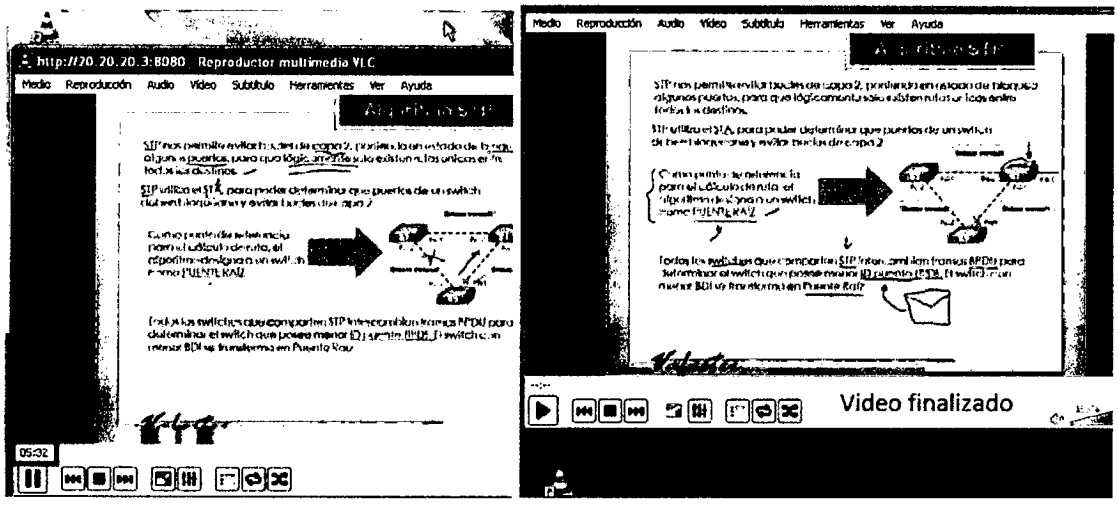


Figura 4.66 Retardo del streaming en el modelo 2 - Next-hop-self (Elaboración Propia)

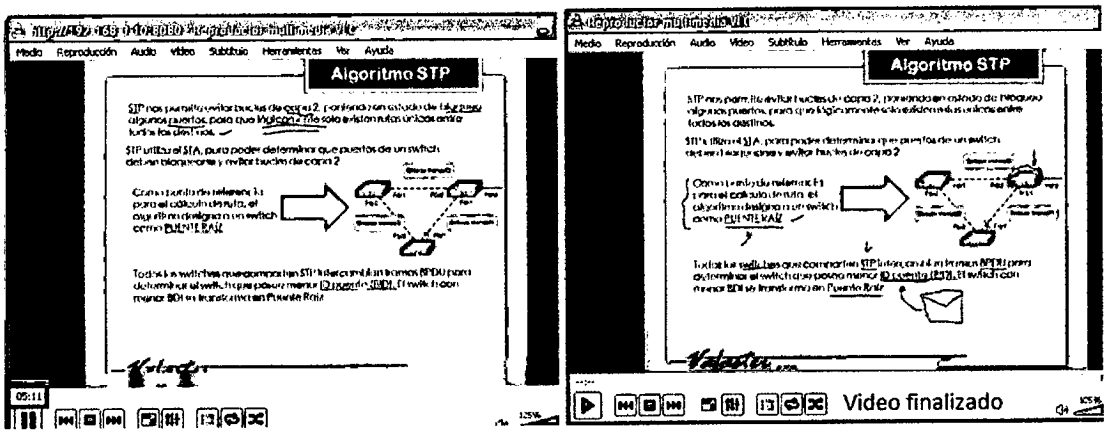


Figura 4.67 Retardo del streaming en el modelo 3 - Redistribute connected (Elaboración Propia)

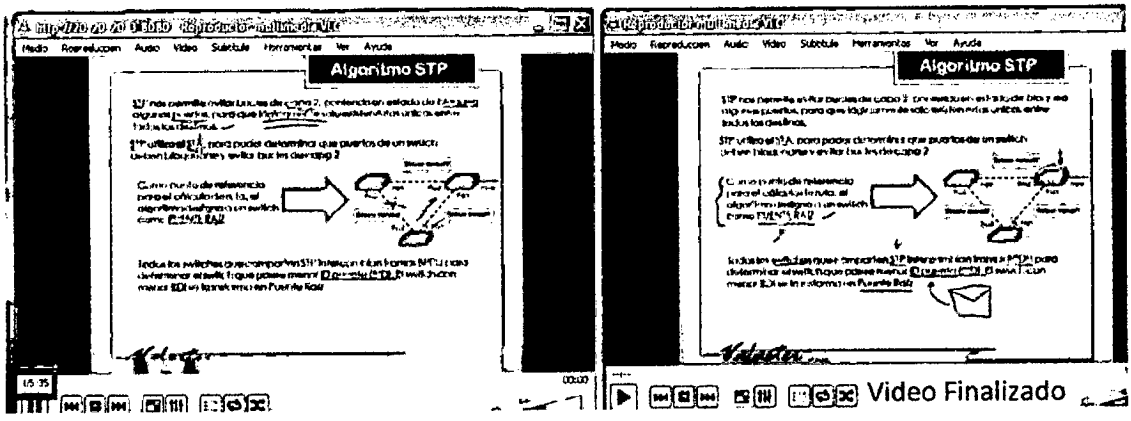


Figura 4.68 Retardo del streaming en el modelo 4 - Multihop MP-eBGP entre Route-Reflectors (RRs) (Elaboración Propia)

Modelo	Tiempo de retardo
Modelo 1	5:35
Modelo 2	5:32
Modelo 3	5:11
Modelo 4	5:35

Tabla 4.23 Comparación del tiempo de convergencia, donde el modelo 3 tiene el tiempo más menor. (Elaboración Propia)

4.1.4 Análisis de los resultados

De las tablas 4.17 y 4.18, obtenemos tiempos de respuestas en promedio igual, por lo cual, no podemos concluir nada. De la tabla 4.19, tenemos que los modelos 1 y 2 tienen "jitter" con promedio iguales, ahora salvo por el modelo 3 que a un bandwidth de 20 Mb/s tiene un valor de jitter de 0, esto se debe al - tal como se muestra en las figuras 4.18, 4.19 y 4.20 – reinicio de sesiones BGP, OSPF y LDP en todos los modelos excepto en el modelo 3, de lo cual se deduce que afecta al rendimiento de la red.

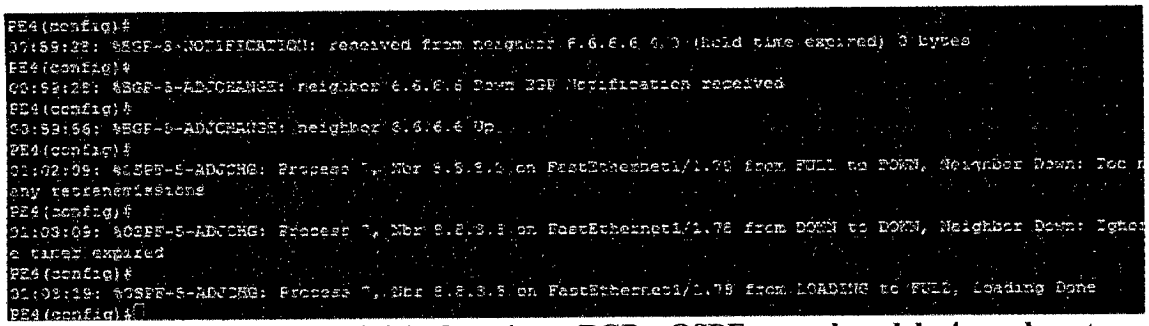


Figura 4.69 Captura de reinicio de sesiones BGP y OSPF para el modelo 4, en el router PE4, cuando se utiliza la herramienta Iperf a 20Mb/s con tráfico UDP durante un tiempo de 180 seg, lo cual afecta en la entrega de los paquetes UDP durante el tiempo señalado.

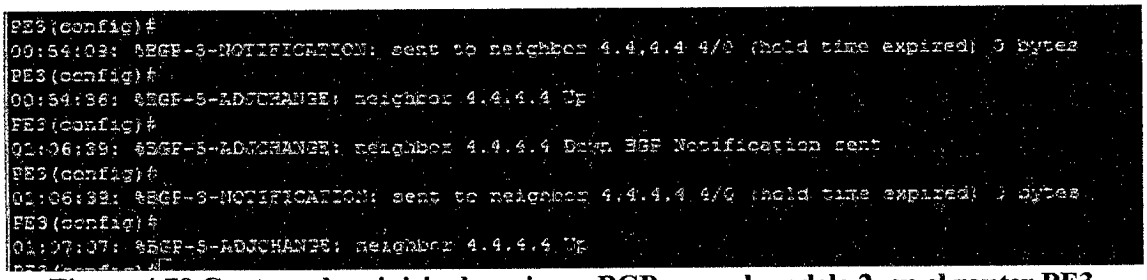


Figura 4.70 Captura de reinicio de sesiones BGP para el modelo 2, en el router PE3, cuando se utiliza la herramienta Iperf a 20Mb/s con tráfico UDP durante un tiempo de 180 seg, lo cual afecta en la entrega de los paquetes UDP durante el tiempo señalado.

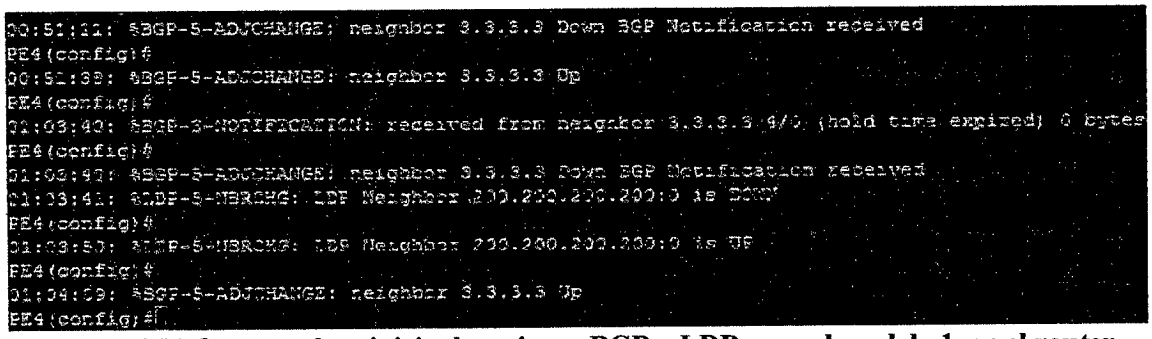


Figura 4.71 Captura de reinicio de sesiones BGP y LDP para el modelo 1, en el router PE4, cuando se utiliza la herramienta Iperf a 20Mb/s con tráfico UDP durante un tiempo de 180 seg, lo cual afecta en la entrega de los paquetes UDP durante el tiempo señalado.

De la Tabla 4.21, tenemos que el menor tiempo de convergencia medido (con herramienta wireshark), son – después del reset BGP- los modelos 2, 3 y 4, pero es el modelo 3 el que tiene poco envío de actualizaciones, ya que la comunicación de los routers ASBR PE2 y PE3 es eBGP

De la Tabla 4.22, se obtuvo que tanto el modelo 3 y 4 tienen el mismo impacto en los routers PE2 y PE3 cuando se hace uso del CPU en los routers mencionados, pero, con

una pequeña diferencia en el router PE3 del modelo 3, ya que para comunicarse con PE2 - pues existe Multihomed - indica al sistema autónomo fuera de nuestra red por cual de mis salidas prefiero que el tráfico externo entre. Y para finalizar, en la Tabla 4.23, el modelo 3 tiene un tiempo de retardo de streaming de 5:11, lo cual es un tiempo aceptable, recordando que si bien es un tráfico TCP, se da prioridad al tráfico streaming, pero, hay que recordar que ha sido de una PC a otra PC, ya que solo se esta estudiando los modelos que puedan, en un futuro, a aplicar criterios tales como RSPV o Tráfico de Ingeniería.

De lo cual se deduce, que el modelo 3 es el ideal ya que, solo se refleja las configuraciones necesarias para implementar esta metodología. Las configuraciones de los routers PE2 y PE3 del modelo 2 son similares a la del modelo 3 de donde se excluye la declaración "next-hop-slef" por "route map" o Multihomed", por lo cual, tiene una gran escalabilidad que brinda esta implementación.

Un punto importante a destacar es la escalabilidad que brinda el modelo 3. Ya que, la configuración entre los routers ASBRs se hace menos engorrosa, lo que hace más factible el incremento de clientes en el enlace. Pues no es necesario modificar la configuración en la conexión entre los proveedores de servicios cada vez que se agreguen clientes, lo cual la convierte en una solución muy escalable.

4.2 Propuesta Técnica

En base a los resultados del análisis de los resultados, se concluyó que el modelo "MP-eBGP entre ASBRs - Redistribute Connected" es el ideal para una implementación sobre Inter-AS VPN utilizando MPls.

Para poder implementar este modelo se necesita equipos que puedan soportar protocolos como BGP, MPLS y VRF que, si bien son protocolos libres, tenemos que considerar que cada fabricante tiene características diferentes en sus respectivos IOS, para ello tenemos escenarios de implementación para equipos del cliente (que son los routers PEs) y en los proveedores de servicio (backbone MPLS).

4.2.1 Recursos Técnicos

En la elección de los routers va a depender de la cantidad de tráfico, si hablamos de una red mediana o algo así; ahora, el tráfico, pero también va a tener sus limitaciones, como todo equipo digamos, si sobrepasamos esas limitaciones que tenga, ya sea de capacidad de forwardeo de tráfico, hardware como tal, pues simplemente ya no va a servir, también depende mucho para qué estemos diseñando, para que cantidad de tráfico, que tipo de servicios estemos mandando; por ejemplo si queremos implementar una red que ahorita digamos quiero nada más implementar voz pero si uno piensa que a dos años ya voy empezar a meter video y voy a empezar a meter mucho tráfico de video, pues pensar en equipos que soporten toda esa cantidad de tráfico, como equipos más grandes que soporten toda esa cantidad de prefijos y toda esa cantidad de procesamientos, ahora si la idea es con quedarnos con nada más con 100 prefijos en mi tabla de ruteo, voy a manejar nada más aplicaciones de datos normales, CTPs cosas por el estilo, pues equipos de menos capacidad pueden servir.

Analizaremos tres marcas tales como CISCO, JUNIPER y HUAWEI, que son las que más predominan en el mercado.

4.2.1.1 CISCO

En lo que es gama para mediana y pequeña empresa tenemos a la serie 7200 de CISCO, en la siguiente tabla se muestra características que ofrece dicha serie.

Características	Beneficios
Capacidad de procesamiento Up to 2 Mpps.	Up to 2 Mpps
Opciones de conectividad máxima.	Reune una variedad de requeriemtos de topología con un amplio rango de puertos densos y opciones de interfaces.
Amplio Servicios	Soporta QoS, seguridad, MPLS, ancho de banda, multiservicio, VoIP, BGP y VRF.
Protección de Inversión	Inversión baja con actualizaciones y capacidad de auto desarrollo.

Tabla 4.24 Características y beneficios de los routers de la serie Cisco 7200

Además de compatibilidad de IOS CISCO que pueden ejecutarse en este equipo.

Nombre de caraterística	Publicación	Información de caraterística
Multiprotocol BGP MPLS VPN	12.0(11)ST 12.2(9)S 12.2(17b)SXA 12.2(27)SBB 12.3(8)T 15.2(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	MPLS VPN consiste en el establecer sitios que serán interconectados a través de una red núcleo proveedora MPLS. En cada sitio, hay una o más routers CEs, que a la vez está unido a una o más Pes. Esta característica reduce el tiempo muerto de una falla de link PE-CE enrutando el tráfico de la PE-salida sobre un trayecto de backup al CE antes de que el BGP reconverga. En 12.2 (33) SRC, esta característica fue introducida en el Cisco 7200 y el Cisco 7600. En 12.2 (33) SB, esta característica estaba disponible en las Cisco 7300 Series y los Cisco 10000 Series Router. Esta característica era integrada en el Cisco IOS Release 15.0 (1) M. Se ha insertado el siguiente comando: **protection local-prefixes**.
MPLS VPN — Convergencia local BGP para 6VPE/6PE	15.0(1)S	Esta característica implementa el MPLS VPN — Convergencia local BGP para el Cisco IOS 6VPE y el Cisco IOS 6PE sobre el MPLS. El siguiente comando fue modificado: **protection local-prefixes**.

Tabla 4.25 Compatibilidad de IOS CISCO en los routers de la serie 7200

4.2.1.2 JUNIPER

En esta marca tenemos todas las siguientes series que soportan MPLS, BGP y VRF.

EX4600
M Series
MX Series
OCX1100
PTX Series
SRX Series

Tabla 4.26 Routers de la serie JUNIPER

La Juniper Networks SRX100 Services Gateway ofrece características que proveen funcionalidades completas y flexibilidad en el acceso seguro a internet e intranet. Los servicios Gateway ofrecen estabilidad, confiabilidad y eficiencia en el enrutamiento IP en adición al soporte switching y conectividad LAN. El dispositivo provee IP Security (IPsec), virtual private network (VPN), y servicios de firewall para pequeña y mediana empresa y sucursales y oficinas remotas.

La SRX100 Services Gateway pueden ser conectados directamente a una red privada tal como una línea arrendada Frame Relay, BGP o Multi Protocol Label Switching (MPLS) o internet público.

Junos OS Software version tested	**Junos OS 12.1X44-D15**
Firewall performance (max)	700 Mbps
IPS performance	75 Mbps
AES256+SHA-1 / 3DES+SHA-1 VPN performance	65 Mbps
Máximo de sesiones simultáneas.	32,000
New sessions/second (sustained, TCP, 3-way)	1,800
Maximum security policies	384

Tabla 4.27 Características de SRX100 Services Gateway

Junos 15.1
Junos 14.2
Junos 14.1
Junos 13.3
Junos 13.2
Junos 15.1

Tabla 4.28 IOs compatible con SRX 100 Services Gateway que soportan los protocolos requeridos

4.2.1.3 HUAWEI

En esta marca tenemos las siguientes series de dicho fabricante:

Routers empresariales de la serie AR3200
Routers empresariales de la serie AR2200
Routers empresariales de la serie AR1200

Tabla 4.29 Routers de la serie HUAWEI

Nos enfocaremos en la serie AR3200. Tenemos las siguientes características:

- Los servicios integrados incluyen conferencias de voz y admiten hasta 500 casillas de correo de voz.
- La monitorización de redes a nivel de paquetes de servicios y el intercambio en caliente dinámico permiten lograr rapidez en la detección de fallos y las copias de seguridad.
- Firewall integrado, IPS y filtrado de URL; compatibilidad con la autenticación de portales, MAC y 802.1x; acceso seguro de VPN IPsec, EVPN, DSVPN, VPN inteligente y A2A.
- BPX, servidor SIP y gateway SIP integrados con interconexiones de NGN/IMS/PBX para los servicios de voz; la función de calidad de experiencia (QoE) de Huawei monitoriza la calidad de voz en tiempo real y administra dinámicamente el jitter de la memoria intermedia, la cancelación de eco y la compensación por pérdida de paquetes a fin de mantener comunicaciones de voz de alta calidad.
- Admite múltiples modos de 3G/LTE inalámbricos de alta velocidad, controladores de acceso inalámbricos y múltiples puntos de acceso para lograr comunicaciones de voces cableadas e inalámbricas sin inconvenientes.

Basic Features	DHCP server/client, PPPoE server/client, PPPoA client, PPPoEoA client, NAT, and sub-interface management
Voice	RTP, SIP, SIP AG, IP PBX/TDM PBX, FXO/FXS, VoIP/conference call, BEST, DISA, and SBC
WLAN (AC)	AP management (AC discovery/AP access/AP management), CAPWAP, WLAN user management, WLAN radio management 802.11a/b/g/n, WLAN QoS (WMM), and WLAN security (WEP/WPA/WPA2/Key management)
LAN	IEEE 802.1P, IEEE 802.1Q, IEEE 802.3, VLAN management, MAC address management, and MSTP
IPv4 Unicast Routing	Routing policy, static route, RIP, OSPF, IS-IS, and BGP
IPv6 Unicast Routing	Routing policy, static route, RIPng, OSPFv3, IS-ISv6, and BGP4+
Multicast	IGMP v1/v2/v3, IGMP-Snooping Version 1/2/3, PIM SM, PIM DM, and MSDP
MPLS	LDP, MPLS L3 VPN, static LSP, dynamic LSP, MPLS TE, IP FRR, LDP FRR, and TE FRR
VPN	IPSec VPN, GRE VPN, DSVPN, L2TP VPN, and Smart VPN
QoS	DiffServ mode, MPLS QoS, priority mapping, traffic policing (CAR), traffic shaping, congestion avoidance (based on IP precedence/DSCP WRED), congestion management (LAN interface: SP/WRR/SP+ WRR WAN interface: PQ/CBWFQ), MQC (traffic classifier, traffic behavior, traffic policy), hierarchical QoS, FR QoS, Smart Application Control (SAC), and Hard QoS
Security	ACL, firewall, 802.1x authentication, MAC address authentication, Web authentication, AAA authentication, RADIUS authentication, HWTACACS authentication, broadcast storm suppression, ARP security, ICMP attack defense, URPF, IP source guard, DHCP snooping, CPCAR, blacklist, and IP source tracing
Management and Maintenance	Upgrade management, device management, web-based GUI, GTL, SNMP Versions 1/2c/3, NTP, CWMP, auto-config, deployment using USB disk, NetConf, and CLI

Tabla 4.30 Especificaciones de los routers de la serie Huawei AR3200

Una de las ventajas con respecto a los demás es que el almacenamiento de la memoria flash puede ser expandidad en una Micro-SD card.

4.2.2 Protocolos y referencias a emplearse

Vamos a tomar como referencia a las normas BGP/MPLS IP Virtual Private Networks (VPNs) (RFC 4364 y 4365). Este documento proporciona una solución a Virtual Private Network (VPN), solución que se describe en [BGP-IP-MPLS-VPN] y otros documentos enumerados en la sección de Referencias. Nos referimos a estos como "BGP / MPLS IP VPN", porque Borde Gateway Protocol (BGP) se utiliza para la distribución de las rutas, y Multiprotocol Label Switching (MPLS) es para indicar que los paquetes de particular necesidad de seguir rutas específicas. Una VPN servicio es proporcionado por un proveedor de servicios (SP) a un cliente (A veces conocida como una empresa). BGP / MPLS IP VPNs son utilizados en situaciones en que:

Sobre El cliente: Utiliza la VPN solo para el transporte de paquetes IP. No quiere administrar una ruta troncal, el cliente podrá usar el enrutamiento dentro de sus sitios, pero desea subcontratar entre el sitio de enrutamiento para la SP. Quiere que el SP para que su encaminamiento de rutas sea completamente transparente para el cliente de la propia ruta. Si el cliente tiene una infraestructura enrutada en sus sitios, no quiere que su sitio algoritmos de enrutamiento deben ser conscientes de cualquier parte de la red principal de SP, que no sea el Provider Edge (PE) routers los sitios a los que se adjuntan.

En particular, el cliente no quiere que su necesidad a los enrutadores, a ser consciente de, ya sea el nativo de la estructura de la columna vertebral SP o una superposición topología de los túneles a través de la columna vertebral SP.

Sobre el proveedor de servicios: Posiblemente (aunque no necesariamente) con MPLS-enabled básico Routers. BGP/MPLS IP Virtual Private Networks (VPNs) (RFC 4364).

4.2.3 Enlaces

Se deben implementar enlaces físicos que interconecten las redes de proveedores y la del cliente. Los enlaces son los siguientes:

Para la conexión entre Proveedores, se empleará un enlace serial pero, hoy en día tenemos la fibra óptica que puede utilizarse con la tecnología Ethernet (FCoE, Fibre Channel over Ethernet), lo que hace más rentable a la hora de su implementación y fácil manejo

Para las conexiones entre el Cliente y cada Proveedor, se emplearán enlaces Fast-Ethernet, tal como se hizo uso en la simulación, donde básicamente todo los enlaces fueron Fast-Ethernet.

4.2.4 Direccionamiento IP

Al ser una VPN, las direcciones IP utilizadas serán privadas. La siguiente tabla muestra los rangos utilizados en esta propuesta para el lado CE(router cliente), PE(router proveedor) y ASBR(routers para interconectar los ASN) .

En lo que respecta al direccionamiento de la backbone MPLS puede ser distinto, ya que, puede utilizarse la infraestructura de un ISP como Viettel Perú SAC, en la cual maneja su propio direccionamiento IP.

Rango	Máscara	Clase	Uso
192.168.1.0	255.255.255.0	C	CLIENTE FINAL ASN 234 A CE1.
192.168.3.0	255.255.255.0	C	CLIENTE FINAL ASN 567 A CE2.
10.10.10.0	255.255.255.0	A	CONEXIÓN CE1 A PE1.
20.20.20.0	255.255.255.0	A	CONEXIÓN CE2 A PE4.
23.23.23.0	255.255.255.0	A	CONEXIÓN ASN 234 A ASN 567.

Tabla 4.31 Direcciones IP

4.2.5 Topología de la red propuesta

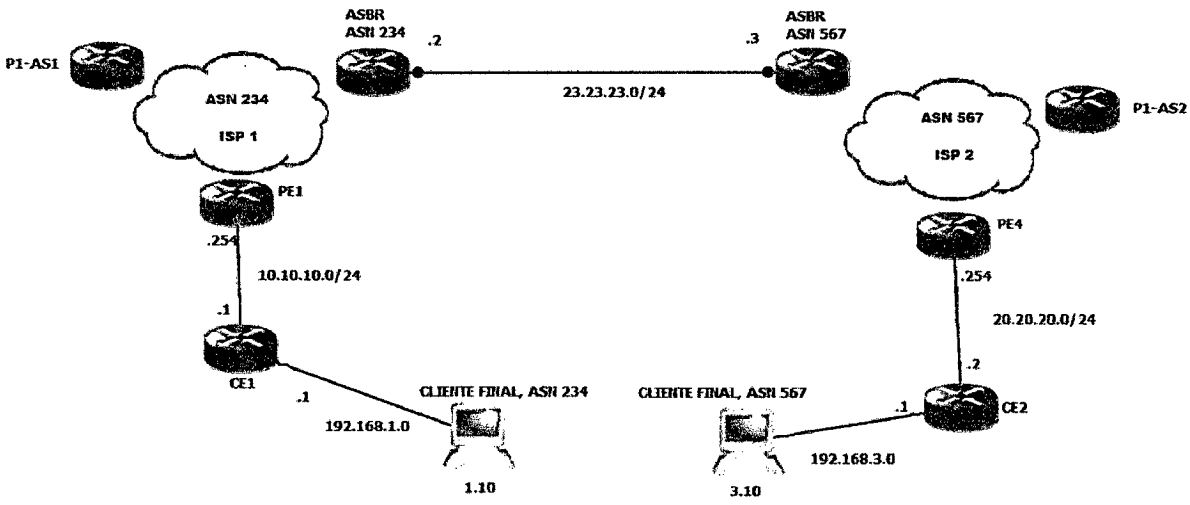


Figura 4.72 Topología propuesta

Como se observó en la última figura, las direcciones propuestas son privadas ya que forman parte de una red que no interactúa directamente con ninguna otra.

4.2.6 Costos económicos

CONCEPTOS	COSTOS UNITARIOS	MARCA	COSTO USD + IGV
CISCO SERIE 7200	US$ 1 500.00	CISCO	1770.00
SRX100 JUNIPER	US$ 1 750.00	JUNIPER	2065.00
AR3200 HUAWEI	US$ 1 300.00	HUWEI	1534.00

Tabla 4.32 Precios solicitados en Telmark S.A.C vía cotización.

Hay que considerar que constantemente los productos cambian en características, actualizaciones lo que produce variaciones de precios.

A la par de esto, considerar que los precios de estos equipos se fijan en moneda del dólar cuya volatilidad depende de factores externos lo cual influye en el precio final. Todos estos equipos tienen una garantía de 02 años y un periodo de entrega máximo de 20 días.

Para la red backbone de MPLS se puede alquilar infraestructuras existentes de los operadores de servicios en el país, tal como Telefónica del Perú, América Móvil y Viettel Peru. O también alquilar la infraestructura del Red Dorsal Nacional de Fibra Óptica que se está ejecutando en paralelo a la realización de esta tesis, cuya novedad es que el concesionario de la RDNFO cobrará una tarifa mayorista de transporte de 27 dólares (impuestos incluidos) por un enlace de 1 Mbps mensual, lo cual las empresas operadoras de Internet o cualquier otra, por fin podrán ver en provincia un mercado potencial para sus operaciones, debido a la política de regulación de precios a cargo de OSIPTEL, asignada a este proyecto.

4.2.7 Beneficios de la propuesta

Una vez que la red esté implementada, se puede ofrecer servicios de Internet dedicado en provincias, a precios entre 40% y 50% menos de los actuales, ya sea a través de fibra óptica, sistema inalámbrico no compartido de punto a punto o el alquiler de infraestructura (fibras oscuras). Y también servicios complementarios, como transmisión de datos, telefonía fija IP, video streaming y seguridad gestionada.

Esta elección se basa en las pruebas realizadas en el capítulo 3, donde se observó que presentaba valores de retardo entre 199 ms para el caso del enlace sin tráfico, y 628 ms en el caso con 20 conexiones generando tráfico simultáneamente. En cuanto al ancho de banda, se obtuvo un rendimiento de 89.84% sin tráfico y de 47.53% con alto tráfico. Estos valores son comparables a los obtenidos en los demás modelos. Sin embargo, este modelo mostró gran capacidad para el procesamiento de información, al no utilizar más del 10% del CPU durante las 3 pruebas y a la vez que el proceso de reset BGP se comparte en los tres router, que son, P1-AS1, PE2 y PE3. Esto es de suma importancia teniendo en cuenta el incremento constante de clientes que buscan contratar un servicio VPN.

A la propuesta técnica también va a depender de las características de la red, qué pasaría si agregamos QoS, tema que no hemos tocado en la presente tesis. Los proveedores con redes muy grandes utilizan equipos GSR, CRS dentro de su CORE por la gran cantidad de prefijos y anchos de banda que pueden llegar a manejar. Como PE's los equipos más usados son 7600 y ASR9k.; de la cantidad de servicios que quieran agregar y de su planeación de crecimiento que se tenga.

Además, el corto tiempo de convergencia obtenido en esta solución, que tuvo un valor máximo de 0.312 ms en el caso más crítico, permite afirmar que en caso de existir eventos que puedan hacer que una sesión BGP caiga, ésta se recuperará rápidamente, reduciendo así el tiempo de indisponibilidad de servicio hacia los clientes.

CONCLUSIONES Y RECOMENDACIONES

Una vez se ha finalizado la propuesta técnica de implementación de una Inter – AS MPLS VPN, teniendo en cuenta que no pretende ser teórico sino un supuesto aproximado a futuras implementaciones de una red MPLS o implementaciones de VPN MPLS, de lo cual, se han obtenido las conclusiones y recomendaciones que se detallan a continuación:

- Se realizo el estudio de cuatro modelos de Inter-AS MPLS VPN con el respectivo análisis de la tasa de reinicios de adyacencias (tales como OSPF, BGP y LDP).
- Se explico en cada modelo el funcionamiento de MPLS, que trabaja en capa 2 y 3 del modelo OSI y para ello se demostró haciendo uso de herramientas que se han detallado en la presente tesis.
- Se reviso los conceptos teóricos de los procesos globales (enrutamiento, reenvío) utilizados en una red sobre la que corre MPLS, así como, el funcionamiento del protocolo BGP que hace posible la comunicación de redes a través de un ASN.
- Se diseño y simulo una topología única para todos los modelos, que sirve para explicar el funcionamiento de los procesos básicos MPLS y BGP, que si bien, el 100% fue simulación, permitio corroborar el funcionamiento de la tecnología para futuros casos reales.
- Se concluyo que el tercer modelo MP-eBGP entre ASBRs - Redistribute Connected es la mejor alternativa por la escalabilidad y calidad de servicio –pese a que no se hizo énfasis en tráfico de ingeniería-, que haciendo uso de "route-map", anuncia las rutas privadas pero no el número del sistema autónomo privado.
- Gracias a la conmutación de etiquetas y al sencillo manejo de la misma se reduce procesamiento en los equipos de la red aumentando la capacidad de manejar un mayor tráfico que en una red IP convencional.
- Para aumentar la seguridad de la información de cada VPN se puede utilizar protocolos de encriptación de datos como IPSec, el cual es utilizado para implementar túneles VPN. Dicha encriptación se aplicará en los routers de borde (PEs y ASBRs), que son el enlace de comunicaciones con otras redes.

REFERENCIAS BIBLIOGRÁFICAS

Ariganello Ernesto & Barrientos Enrique (2010). *Redes Cisco: CCNP a fondo, guía de estudio para profesionales.* Madrid, España: Ra-Ma Editorial.

Cisco Systems. (2006). *Implementing Cisco MPLS volumen 1 versión 2.2 Student guide.* Recuperado de https://renatazuccarello.files.wordpress.com/2009/06/mpls22sg_vol-11.pdf

Cisco Systems. (2006). *Inter-Autonomous Systems for MPLS VPNs.* [Presentación en PDF]. Recuperado de ftp://ftp.sakhalin.ru/docs/cisco/interas-mpls-vpn.pdf

Cisco Systems. (2013). *MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T.* [Presentación en PDF]. Recuperado de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book.pdf

Chica Bermúdez, Eduardo Xavier. & Samaniego Palacios, Carlos Patricio. (2008). *Análisis, diseño y simulación de una red MPLS de un portador nacional que permita comparar los servicios de VPN capa 2 y capa 3.* (Tesis de Grado). Escuela Superior Politécnica del Litoral. Ecuador, Guayaquil. Recuperado de http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-83745.pdf

García Girón, Giancarlo. (2009). P*ropuesta de migración de la red NGN de una operadora implementada en IP hacia MPLS.* (Tesis de Grado). Pontificia Universidad Católica del Perú. Perú, Lima. Recuperado de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1063/GARCIA_GIRON_GIANCARLO_MIGRACION_NGN_HACIA_MPLS.pdf?sequence=1

Gómez Valdivia, Javier Rafael. & Moliner Peña, Carmen. (2005). *MPLS y su aplicación en Redes Privadas Virtuales (L2VPNS y L3VPNS).* LACCET' – Information Technology Track. 8-10, Cartagena de Indias, COLOMBIA. Recuperado de http://www.laccei.org/LACCEI2005-Cartagena/Papers/IT083_MolinerPena.pdf

Gonzáles, Francisco Javier. (2014). *Redes-MPLS.* [Diapositivas de PowerPoint]. Telefónica. Jefatura Plataformas Datos e Internet. Recuperado de http://es.slideshare.net/Randyatencia/redes-mpls-introduccion

González Bojorges, Axel Iván. (2012). *Redunam Metropolitana: Diseño, pruebas y prelicitación.* (Tesis de Grado). Universidad Nacional Autónoma de México. México, D. F. Recuperado de http://docplayer.es/456680-Redunam-metropolitana-diseno-pruebas-y-prelicitacion-tesis-ingeniero-en-telecomunicaciones-axel-ivan-gonzalez-bojorges.html

González Carrasco, Álvaro. (2011). *Integración y optimización de redes MPLS: Un caso práctico.* (Tesis de Grado). Universidad Carlos III de Madrid. España, Madrid. Recuperado de http://e-archivo.uc3m.es/bitstream/handle/10016/20236/PFC_Alvaro_Gonzalez_Carrasco.pdf?sequence=1

Haas, Hebert. (2005). *MPLS Inter – AS VPN, Interconnecting MPLS Networks.* [Presentación en PDF]. Recuperado de http://www.perihel.at/2/basics/36-MPLS-02-VPN-Inter-AS.pdf

Herrera Merchán, Fabricio Fernando. & Hinojosa López, Mayra Alexandra. (2009). *Diseño de una red MPLS utilizando el protocolo IPV6 para proveedores de servicios de telecomunicaciones.* (Tesis de Grado). Escuela Politécnica Nacional. Ecuador, Quito. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/1718/1/CD-2327.pdf

Huertas, Jose M. (2012). *InterAS VPN: Option 10A (Back to Back VRF).* Recuperado de https://blog.initialdraft.com/archives/4209/.

Kollar, Stefan. (2009). *I-AS MPLS Solutions.* [Presentación en PDF]. Consulting System Engineer. Recuperado de http://www.cisco.com/web/SK/expo2009/docs/C3_InterAS_MPLSSolutions_StefanKollar.pdf

Marchán, J. & Yánez, D. (2008). *Estudio y Diseño para la migración de una red Gigabit Ethernet de datos de una empresa portadora de servicios a la tecnología MPLS.* (Tesis de Grado). Escuela Politécnica Nacional. Ecuador, Quito. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/1024/1/CD-1464%282008-05-22-08-48-01%29.pdf

Martínez Marciales, Rocy Y. (2008). *Estudio y pruebas del comportamiento de los mecanismos de reserva en una red MPLS.* (Tesis de Grado). Universidad Simón Bolívar. Venezuela, Caracas. Recuperado de http://159.90.80.55/tesis/000139537.pdf

Mahmoud, Mohammed (2008). *Inter-AS MPLS VPN – The whole story.* Recuperado de http://www.networkers-online.com/blog/2008/12/inter-as-mpls-vpn-the-whole-story-updated-dec-2008/

Orozco Lara, Fausto Raúl. (2014). *Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil.* (Tesis de Grado). Universidad Católica de Santiago de Guayaquil. Ecuador, Guayaquil. Recuperado de http://repositorio.ucsg.edu.ec/bitstream/123456789/2198/1/T-UCSG-POS-MTEL-23.pdf

Pandya, Sangita & Rakotoranto, Hari. (2007). *I-AS MPLS VPN Solutions.* [Presentación en PDF]. Consulting System Engineer. Recuperado de http://www.webtorials.com/main/resource/papers/FutureNet2008/Session20.pdf

Reuter, A. Jiménez, M. (2013). *Diseño del Backbone de la red óptica metropolitana con tecnología MPLS para un Proveedor de Servicios de Internet dentro del Distrito Metropolitano de Quito.* Revista Politécnica. 32(2), 23-32. Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000/5174/3/CD-4555.pdf

Tapasco Garcia, Martha Odilia. (2008). *MPLS, El presente de las redes IP.* (Tesis de Grado). Universidad Tecnológica de Pereira. Colombia, Pereira. Recuperado de http://repositorio.utp.edu.co/dspace/bitstream/11059/1311/1/0046T172.pdf

ANEXO 1: IPV6 SOBRE MPLS VPN

1. Introducción a IPv6

Una dirección IPv6 está formada por 128 bits. Las direcciones se clasifican en diferentes tipos: unicast, multicast y anycast.

2. Formato

Las direcciones unicast generalmente se dividen en dos grupos lógicos: los primeros 64bits identifican el prefijo de red (routing-prefix o subnet prefix), y son usados para encaminamiento; los últimos 64 bits identifican el interface de red del host (interfaceID).

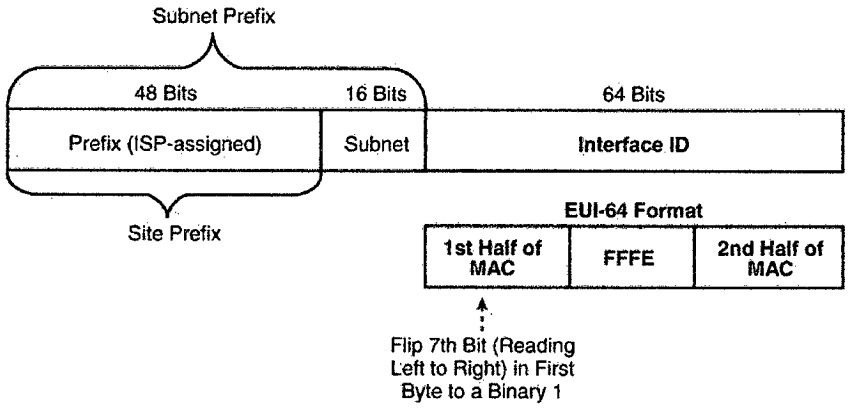


Figura 2.1 Formato dirección IPv6

Una dirección IPv6 se representa mediante ocho grupos de cuatro dígitos hexadecimales, cada grupo representando 16 bits (dos octetos). Los grupos se separan mediante dos puntos (:). Un ejemplo de dirección IPv6 podría ser:

2001:0000:85a3:0000:0000:8a2e:0370:7334

Esta representación completa puede ser simplificada de varias maneras, eliminando partes de la representación.

- Los ceros iniciales de cada grupo pueden omitirse, aunque cada grupo debe contener al menos un dígito hexadecimal.
- Uno o más grupos de ceros pueden ser sustituidos por dos puntos. Esta sustitución puede realizarse únicamente una vez en la dirección. En caso contrario, obtendríamos una representación ambigua. Si pueden hacerse varias sustituciones, debemos hacer la de mayor número de grupos; si el número de grupos es igual, debemos hacer la situada más a la izquierda. Con esta regla, reduciríamos la dirección del ejemplo a: 2001:0:85a3::8a2e:370:7334.

3. Ambitos

Toda dirección IPv6, excepto la dirección indefinida (::), tiene un "ámbito" (scope en inglés), que determina en qué partes de la red es válida. En direccionamiento unicast:

- Las direcciones link-local y la dirección de loopback tienen ámbito de enlace local, es decir, deben ser usadas en la red directamente conectada. Una dirección IPv6 Link-Local comienza con el prefijo FE80::/10 (los primeros 10 bits), luego los bits del 11 hasta 64 (los siguientes 54 bits) se configuran con valores de ceros. Los restantes 64 bits son de interfaceID. Estas direcciones usan por lo tanto el formato siguiente: FE80 :: InterfaceID.
- Las direcciones Unique Local Address (ULA) se utilizan para comunicaciones locales. Son enrutables sólo dentro de un ámbito cooperativo (similar a los rangos de direcciones privadas 10/8, 172.16/12, y 192.168/16 en IPv4). Las direcciones incluyen una secuencia pseudoaleatoria en el routing-prefix para minimizar el riesgo de conflictos en la interconexión de plataformas diferentes o si los paquetes se desvían a Internet (son únicas en todo el mundo).
- El resto de direcciones, excepto aquellas privadas o reservadas, tienen ámbito global, que significa que son mundialmente enrutables y pueden ser usadas para conectarse a direcciones de ámbito global en cualquier lugar.

4. Metodos de configuración de IPv6

Hay dos maneras para configurar una IPv6:

- Statefull es cuando se asigna manualmente o bien cuando se obtiene de un servidor DHCPv6 (junto a otros paramentros como Gateway, nombre, dominio, etc.).
- Stateless es cuando se configura automáticamente (autoconfiguración). El routing-prefix de la dirección global se obtiene de un router conectado a la misma red a través de la nueva funcionalidad Network Discovery y se completa con un interfaceID formato de la conversión de la MAC a 64 bits. Juntamente a un routing-prefix global, se envía también una ruta para salir de la red. De la misma manera, el routing-prefix de la dirección link-local será fe800::/64 y el interfaceID de la conversión a 64 bits de la MAC de la interfaz. Opcionalmente, el router puede enviar también un routing-prefix ULA si este se está usando en este ámbito.

5. MPLS VPN sobre IPv6

Son múltiples las técnicas disponibles para integrar servicios IPv6 en redes: podría ser una red puramente IPv6, una red doble pila IPv4-IPv6 ejecutándose en paralelo, o aprovechar un backbone MPLS/IPv4 existente (como es el caso de la solución que se propone más adelante). Estas soluciones, (despliegue de IPv6) son viables cuando la cantidad de tráfico IPv6 y los ingresos generados están emparejados con las inversiones y los riesgos asumidos.

La implementación de Cisco IPv6 Provider Edge router sobre MPLS se llama 6PE, y permite a sitios IPv6 comunicarse entre sí a través de una red MPLS IPv4 utilizando MPLS Label Switched Paths (LSPs): esta función se basa en una extensión del multiprotocolo Border Gateway Protocol (BGP), y requiere una configuración de red IPv4 en el provider edge router (PE) para intercambiar información de alcanzabilidad IPv6, adicionando una etiqueta MPLS para cada address prefix IPv6 que se anuncia.

Esto es: los routers multiprotocolo 6PE utilizan BGP para intercambiar información de accesibilidad con otros dispositivos 6PE dentro del dominio MPLS y para distribuir etiquetas IPv6 entre ellos. Todos los routers 6PE y de núcleo dentro del dominio MPLS IPv4 comparten un protocolo de borde interno IPv4 (Internal Gateway Protocol - IGP), tales como OSPF O EIGRP.

Los routers de borde están configurados para ser de doble pila (ejecutar IPv4 e IPv6), y utilizarla dirección IPv4 mapeada a IPv6 para el intercambio de prefijos IPv6. En la figura 5.1, los routers 6PE están configurados como doble pila capaz de encaminar el tráfico IPv4 e IPv6. Cada router 6PE esta configurado para ejecutar LDP (Label Distribution Protocol), TDP (Tag Distribution Protocol), o RSVP (Resource Reservation Protocol); este último para el caso que se haya configurado la ingeniería de tráfico para vincular etiquetas IPv4.

La figura 5.1 ilustra el funcionamiento de 6PE:

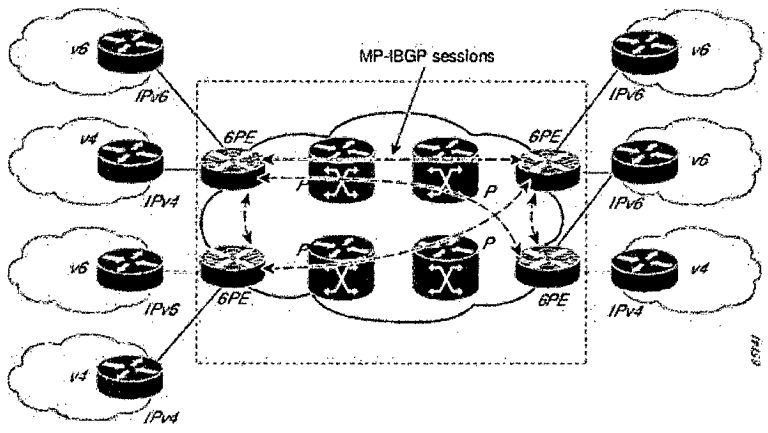


Figura 5.1 6PE – IGP

Las interfaces de los routers 6PE conectadas al router CE pueden ser configuradas para reenviar el tráfico IPv6, IPv4, o ambos tipos de tráfico en función de los requisitos del cliente. Los routers 6PE IPv6 anuncian información de accesibilidad aprendida de sus compañeros 6PE sobre la nube MPLS. Los proveedores de servicios pueden delegar un prefijo IPv6 a través de la infraestructura 6PE, de esta manera, no hay impacto en un router CE.

Los routers P en el núcleo de la red no son conscientes de que se están cambiando los paquetes IPv6. Los routers de núcleo están configurados para soportar MPLS y el mismo IGP IPv4 como los routers PE para establecer accesibilidad interna en el interior de la nube MPLS. Los routers del núcleo también utilizan LDP, TDP, o RSVP para la unión de etiquetas IPv4. Implementar la funcionalidad Cisco 6PE, no tendrá ningún impacto en los dispositivos del núcleo MPLS, dado que dentro de la red MPLS, el tráfico IPv6 se reenvía mediante la conmutación de etiquetas, haciendo que el tráfico IPv6 sea transparente para el núcleo. No se requieren métodos de túneles IPv6 sobre IPv4 o encapsulación de capa 2.

5.1 Configuración y pruebas funcionales en topología con IPv6

Dado que en nuestra topología ya tenemos el protocolo OSPF ejecutándose, a continuación tenemos que iniciar el protocolo 6PE en los routers de borde del backbone. El proceso es muy sencillo: los routers 6PE (R1 y R4) se configuran para el tráfico IPv4 e IPv6.

Entonces, los routers 6PE tienen que:

1. Participar en el protocolo de pasarela interior IPv4 para establecer la accesibilidad interna dentro de la nube MPLS: en el ejemplo que usaremos, tenemos declaradas las interfaces IPv4 con OSPFv2 como IGP.

2. Participar en LDP o TDP para la unión de etiquetas IPv4 como LDP.

3. Ejecutar Multi-Protocol iBGP (MP-iBGP) para anunciar disponibilidad de IPv6 y distribuir aggregate-labels IPv6.

4. Ejecutar MP-eBGP, un IGP IPv6 o encaminamiento estático en routers CE para anunciar prefijos IPv6 aprendidos de sus peers sobre la nube MPLS.

A continuación presentaremos, como parte de la solución propuesta, los archivos de configuración (running-config) 6PE de los routers de borde PE1 y PE2, y de los routers Cliente CE1 Y CE2 correspondientes a la topología presentada en la figura 5.2

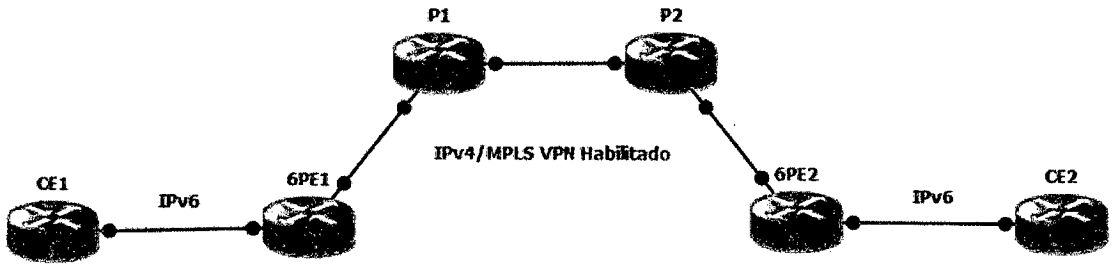


Figura 5.2 MPLS VPN sobre IPV6

5.1.1 Configuración VRF

CE1
ipv6 unicast-routing ipv6 cef interface Serial 0/0 ipv6 address 2001:1::1/124 interface Loopback 0
CE2
ipv6 unicast-routing ipv6 cef interface Serial 0/0 ipv6 address 2001:2::1/124 interface Loopback 0 ipv6 address ABCD::2/128
6PE1
ipv6 unicast-routing ipv6 cef mpls label protocol ldp mpls ldp router-id Loopback 0 force **vrf definition CUST1** **rd 1:1** **!** **address-family ipv6** **route-target import 1:1** **route-target export 1:1** **exit-address-family** ! interface Serial 0/0 **vrf forwarding CUST1** ipv6 address 2001:1::2/124

```
!
interface Loopback 0
 ip address 1.1.1.1 255.255.255.255
 ip ospf 1 area 0
```

6PE2

```
ipv6 unicast-routing

ipv6 cef

mpls label protocol ldp

mpls ldp router-id Loopback 0 force

vrf definition CUST1
 rd 1:1
 !
 address-family ipv6
 route-target import 1:1
 route-target export 1:1
 exit-address-family
!
interface Serial 0/0
 vrf forwarding CUST1
 ipv6 address 2001:2::2/124
!
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
 ip ospf 1 area 0
```

5.1.2 Configuración de (MP-BGP)

Dirección familiar VPNv6 se configura en 6VPE routers para la conexión BGP. Hay una conexión eBGP entre el 6VPE y los routers CE.

CE1

```
router bgp 65101

 neighbor 2001:1::2 remote-as 100

address-family ipv6

 neighbor 2001:1::2 activate

 network ABCD::1/128

 exit-address-family
```

6PE1

```
router bgp 100

 neighbor 3.3.3.3 remote-as 100

 neighbor 3.3.3.3 update-source Loopback 0

 address-family vpnv6

 neighbor 3.3.3.3 activate
exit-address-family
```

address-family ipv6 vrf CUST1
neighbor 2001:1::1 remote-as 65101
neighbor 2001:1::1 activate
redistribute connected
exit-address-family!

CE2

router bgp 65102

neighbor 2001:2::2 remote-as 100

address-family ipv6

neighbor 2001:2::2 activate

network ABCD::2/128

exit-address-family

6PE2

router bgp 100

neighbor 1.1.1.1 remote-as 100

neighbor 1.1.1.1 update-source Loopback 0

address-family vpnv6
neighbor 1.1.1.1 activate
exit-address-family

address-family ipv6 vrf CUST1
neighbor 2001:2::1 remote-as 65102
neighbor 2001:2::1 activate
redistribute connected
exit-address-family

Verificación

BGP Next-Hop Address

```
6PE2#
show bgp vpnv6 unicast vrf CUST1
BGP table version is 30, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf CUST1)
*>i2001:1::/124     ::FFFF:1.1.1.1           0    100      0 ?
*> 2001:2::/124     ::                       0         32768 ?
*>iABCD::1/128      ::FFFF:1.1.1.1           0    100      0 65101 i
*> ABCD::2/128      2001:2::1                0             0 65102 i

6VPE2# show bgp vpnv6 unicast vrf CUST1 ABCD::1/128
BGP routing table entry for [1:1]ABCD::1/128, version 30
Paths: (1 available, best #1, table CUST1)
  Advertised to update-groups:
        2
  65101
```

```
    ::FFFF:1.1.1.1 (metric 3) from 1.1.1.1 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/20
```

Imposición de etiquetas

Cuando un router 6PE recibe un paquete de un router CE vecino, busca la dirección de destino del paquete IPv6 en la tabla VRF correspondiente a ese router CE. Esto le permite encontrar una ruta VPNv6. La ruta VPNv6 tiene una etiqueta asociada MPLS (etiqueta superior) y una etiqueta siguiente BGP-Hop asociado (etiqueta de la parte inferior).

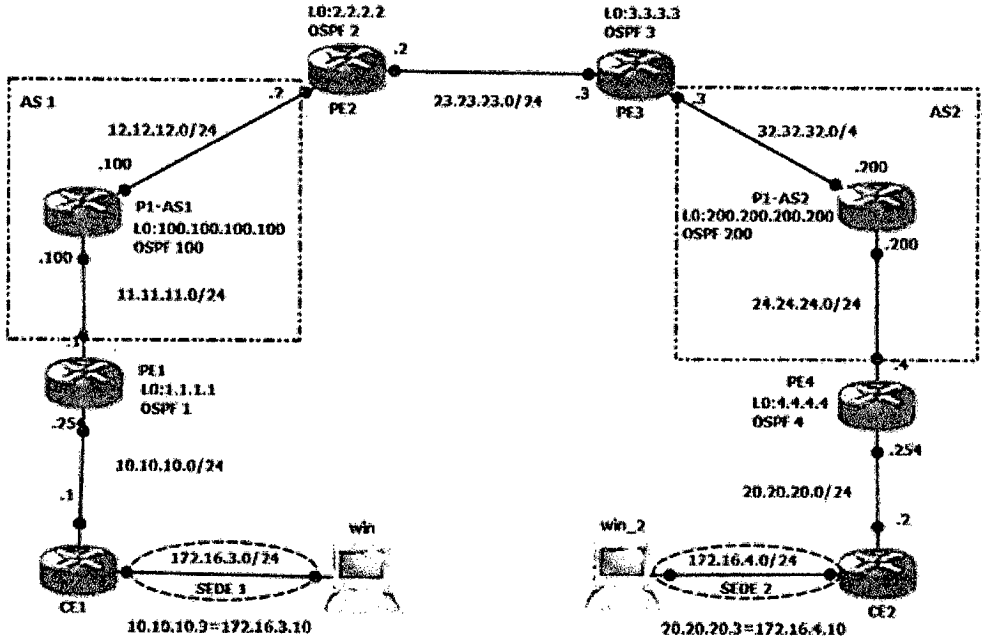
```
6VPE2# show bgp vpnv6 unicast vrf CUST1 ABCD::1/128
BGP routing table entry for [1:1]ABCD::1/128, version 30
Paths: (1 available, best #1, table CUST1)
  Advertised to update-groups:
        2
  65101
    ::FFFF:1.1.1.1 (metric 3) from 1.1.1.1 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/20

6VPE2#
show ip cef 1.1.1.1
1.1.1.1/32
  nexthop 10.2.2.1 FastEthernet2/0 label 16

6VPE2#
show ipv6 cef vrf CUST1 ABCD::1/128 detail
ABCD::1/128, epoch 0
  recursive via 1.1.1.1 label 20
    nexthop 10.2.2.1 FastEthernet2/0 label 16
```

Prefijos IPv6 anunciados para routers CE

El comando show ipv6 route bgp muestra las rutas BGP aprendidas por el router.

```
CE1# show ipv6 route bgp
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
B   2001:2::/124 [20/0]
     via FE80::C808:17FF:FE2C:0, Serial0/0
B   ABCD::2/128 [20/0]
     via FE80::C808:17FF:FE2C:0, Serial0/0
CE2# show ipv6 route bgp
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
B   2001:1::/124 [20/0]
     via FE80::C809:14FF:FEB4:0, Serial0/0
B   ABCD::1/128 [20/0]
     via FE80::C809:14FF:FEB4:0, Serial0/0
```

ANEXO 2: DIRECCIONAMIENTO IP



Esquema de topología en GNS3

EQUIPO	INTERFAZ	IP ADDRESS	RED
CE1	F0/1	172.16.3.1/24	CLIENTE
	F1/0	10.10.10.1/24	
PE1	F1/1	11.11.11.1/24	PROVEEDOR AS 1
	F1/0	10.10.10.254/24	
P1-AS1	F1/1	12.12.12.100/24	PROVEEDOR AS 1
	F1/0	11.11.11.100/24	
PE2	F1/1	23.23.23.2/24	PROVEEDOR AS 1
	F1/0	12.12.12.2/24	
PE3	F1/1	32.32.32.3/24	PROVEEDOR AS2
	F1/0	23.23.23.3/24	
P1-AS2	F1/1	24.24.24.200/24	PROVEEDOR AS2
	F1/0	32.32.32.200/24	
PE4	F1/1	20.20.20.254/24	PROVEEDOR AS2
	F1/0	24.24.24.4/24	
CE2	F1/0	20.20.20.2/24	CLIENTE
	F0/0	172.16.4.1/24	

Tabla 2.1: Esquema de direccionamiento IP de la red

ANEXO 3: CONFIGURACIONES

Modelo 1: Back-to-Back VRFs

Configuración CE1

CE1

```
hostname CE1

no cdp run

interface FastEthernet1/0
 no shut
 ip address 10.10.10.1 255.255.255.0
 exit

interface fastethernet0/1
 no shut
 ip add 172.16.3.1 255.255.255.0
 exit

interface FastEthernet1/0
 ip nat out
 exit

interface fastethernet0/1
 ip nat ins
 exit

ip route 0.0.0.0 0.0.0.0 10.10.10.254
ip nat inside source static 172.16.3.10 10.10.10.3
```

Configuración PE1

PE1

```
hostname PE1
no cdp run

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 exit

interface FastEthernet1/0
 ip vrf forwarding BLUE
 ip address 10.10.10.254 255.255.255.0
 no shut
 exit

interface FastEthernet1/1
 ip address 11.11.11.1 255.255.255.0
 mpls ip
 no shut
 exit
mpls label protocol ldp
mpls label range 30 50
```

```
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 11.11.11.0 0.0.0.255 area 0
 exit

router bgp 1
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 1
 neighbor 2.2.2.2 update-source Loopback0

  address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 exit-address-family

  address-family ipv4 vrf BLUE
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 exit
```

Configuración P1-AS1

P1-AS1

```
hostname P1-AS1

no cdp run

interface Loopback0
 ip address 100.100.100.100 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 11.11.11.100 255.255.255.0
  mpls ip
 no shut
 exit

interface FastEthernet1/1
 ip address 12.12.12.100 255.255.255.0
 mpls ip
 no shut
 exit

mpls label protocol ldp
mpls label range 60 80

router ospf 100
 router-id 100.100.100.100
 log-adjacency-changes
 network 11.11.11.0 0.0.0.255 area 0
 network 12.12.12.0 0.0.0.255 area 0
 network 100.100.100.100 0.0.0.0 area 0
 exit
```

Configuración PE2

PE2

```
hostname PE2

no cdp run

mpls label protocol ldp
mpls label range 90 110

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 12.12.12.2 255.255.255.0
 mpls ip
 no shut
 exit

interface FastEthernet1/1
 ip vrf forwarding BLUE
 ip address 23.23.23.2 255.255.255.0
 no shut
 exit

router ospf 2
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.255 area 0
 exit

router bgp 1
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source Loopback0

 address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 send-community extended
 exit-address-family

 address-family ipv4 vrf BLUE
 redistribute connected
 redistribute static
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
 exit

ip route vrf BLUE 0.0.0.0 0.0.0.0 23.23.23.3
```

Configuración PE3

PE3

```
hostname PE3

no cdp run

mpls label protocol ldp
mpls label range 30 50

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 exit

interface FastEthernet1/0
 ip vrf forwarding BLUE
 ip address 23.23.23.3 255.255.255.0
 no shut
 exit

interface FastEthernet1/1
 ip address 32.32.32.3 255.255.255.0
 mpls ip
 no shut
 exit

router ospf 3
 router-id 3.3.3.3
 netw 32.32.32.0 0.0.0.255 area 0
 netw 3.3.3.3 0.0.0.0 area 0
 exit

router bgp 2
 bgp router-id 3.3.3.3
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 2
 neighbor 4.4.4.4 update-source Loopback0

 address-family vpnv4
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 exit-address-family

 address-family ipv4 vrf BLUE
 redistribute connected
 redistribute static
 default-information originate
 no auto-summary
 no synchronization
 exit-address-family
 exit

ip route vrf BLUE 0.0.0.0 0.0.0.0 23.23.23.2
```

Configuración P1-AS2

P1-AS2

```
hostname P1-AS2

no cdp run

mpls label protocol ldp
mpls label range 60 80

interface Loopback0
 ip address 200.200.200.200 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 32.32.32.200 255.255.255.0
 mpls ip
 no shut
  exit

interface FastEthernet1/1
 ip address 24.24.24.200 255.255.255.0
 mpls ip
 no shut
 exit

router ospf 200
 router-id 200.200.200.200
 netw 32.32.32.0 0.0.0.255 area 0
 netw 24.24.24.0 0.0.0.255 area 0
 netw 200.200.200.200 0.0.0.0 area 0
 exit
```

Configuración PE4

PE4

```
hostname PE4
no cdp run

mpls label protocol ldp
mpls label range 90 110

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
  ip address 4.4.4.4 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 24.24.24.4 255.255.255.0
 mpls ip
 no shut
 exit

interface FastEthernet1/1
 ip vrf forwarding BLUE
```

```
 ip address 20.20.20.254 255.255.255.0
 no shut
 exit

router ospf 4
 router-id 4.4.4.4
 netw 24.24.24.0 0.0.0.255 area 0
 netw 4.4.4.4 0.0.0.0 area 0
 exit

router bgp 2
 bgp router-id 4.4.4.4
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 2
 neighbor 3.3.3.3 update-source Loopback0

  address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family

 address-family ipv4 vrf BLUE
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 exit
```

Configuración CE2

CE2

```
hostname CE2

no cdp run

interface FastEthernet1/0
 ip address 20.20.20.2 255.255.255.0
 no shut
 ip nat out
 exit

interface FastEthernet 0/0
 ip address 172.16.4.1 255.255.255.0
 no shut
 ip nat insi
 exit

ip route 0.0.0.0 0.0.0.0 20.20.20.254
access-list 1 permit 172.16.0.0 0.0.255.255
ip nat inside source list 1 int fa 1/0 overload
```

Modelo 2: MP-eBGP entre ASBRs - Next-hop-self

Configuración CE1

CE1

```
hostname CE1

interface FastEthernet1/0
 no shut
```

```
 ip address 10.10.10.1 255.255.255.0
 exit

interface fastethernet0/1
 no shut
 ip add 172.16.3.1 255.255.255.0
 exit

interface FastEthernet1/0
 ip nat out
 exit

interface fastethernet0/1
 ip nat ins
 exit

ip route 0.0.0.0 0.0.0.0 10.10.10.254
ip nat inside source static 172.16.3.10 10.10.10.3

no cdp run
```

Configuración PE1

PE1

```
hostname PE1

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 exit

interface FastEthernet1/0
 ip vrf forwarding BLUE
 ip address 10.10.10.254 255.255.255.0
 no shut
 exit

interface FastEthernet1/1
 ip address 11.11.11.1 255.255.255.0
 mpls ip
 no shut
 exit

mpls label range 30 50

router ospf 1
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 11.11.11.0 0.0.0.255 area 0
 exit

router bgp 1
 no synchronization
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
```

```
neighbor 2.2.2.2 remote-as 1
neighbor 2.2.2.2 update-source Loopback0

address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
exit-address-family

address-family ipv4 vrf BLUE
redistribute connected
 no auto-summary
no synchronization
exit-address-family
exit

no cdp run
```

Configuración P1-AS1

P1-AS1

```
hostname P1-AS1
no cdp run

interface Loopback0
 ip address 100.100.100.100 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 11.11.11.100 255.255.255.0
 no shut
 mpls ip
 exit

mpls label range 60 80

interface FastEthernet1/1
 ip address 12.12.12.100 255.255.255.0
 no shut
 mpls ip
 exit

router ospf 100
 router-id 100.100.100.100
 log-adjacency-changes
 network 11.11.11.0 0.0.0.255 area 0
 network 12.12.12.0 0.0.0.255 area 0
 network 100.100.100.100 0.0.0.0 area 0
 exit
```

Configuración PE2

PE2

```
hostname PE2

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 12.12.12.2 255.255.255.0
 mpls ip
```

```
 no shut

 exit

interface FastEthernet1/1
 ip address 23.23.23.2 255.255.255.0
 mpls bgp forwarding
 no shut

 exit

mpls label range 90 110

router ospf 3
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 12.12.12.0 0.0.0.255 area 0

 exit

router bgp 1
 no synchronization
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes

 neighbor 23.23.23.3 remote-as 2
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source Loopback0

 address-family vpnv4
 neighbor 23.23.23.3 activate
 neighbor 23.23.23.3 send-community extended
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 next-hop-self
 neighbor 1.1.1.1 send-community extended
 exit-address-family

 exit

no cdp run
```

Configuración PE3

PE3

```
hostname PE3

interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 23.23.23.3 255.255.255.0
 mpls bgp forwarding
 no shut
 exit

interface FastEthernet1/1
 ip address 32.32.32.3 255.255.255.0
```

```
 mpls ip
 no shut
 exit

mpls label range 30 50

router ospf 3
 router-id 3.3.3.3
 netw 3.3.3.3 0.0.0.0 area 2
 netw 32.32.32.0 0.0.0.255 area 2
 exit

router bgp 2
 no synchronization
 bgp router-id 3.3.3.3
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor 23.23.23.2 remote-as 1
 neighbor 4.4.4.4 remote-as 2
 neighbor 4.4.4.4 update-source Loopback0

 address-family vpnv4
 neighbor 23.23.23.2 activate
 neighbor 23.23.23.2 send-community extended
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 next-hop-self
 neighbor 4.4.4.4 send-community extended
 exit-address-family
 exit

no cdp run
```

Configuración P1-AS2

P1-AS2

```
hostname P1-AS2

interface Loopback0
 ip address 200.200.200.200 255.255.255.255
 EXIT

interface FastEthernet1/0
 ip address 32.32.32.200 255.255.255.0
no shut
 mpls ip
 EXIT

interface FastEthernet1/1
 ip address 24.24.24.200 255.255.255.0
 mpls ip
 no shut
 exit

mpls label range 60 80

router ospf 200
 router-id 200.200.200.200
 netw 32.32.32.0 0.0.0.255 area 2
 netw 24.24.24.0 0.0.0.255 area 2
 netw 200.200.200.200 0.0.0.0 area 2
```

```
exit

no cdp run
```

Configuración PE4

PE4

```
hostname PE4

ip vrf BLUE
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 exit

interface FastEthernet1/0
 ip address 24.24.24.4 255.255.255.0
 no shut
 mpls ip
 exit

interface FastEthernet1/1
 ip vrf forwarding BLUE
 ip address 20.20.20.254 255.255.255.0
 no shut
 exit

mpls label range 90 110

router ospf 4
 router-id 4.4.4.4
 netw 24.24.24.0 0.0.0.255 area 2
 netw 4.4.4.4 0.0.0.0 area 2
 exit

router bgp 2
 no synchronization
 bgp router-id 4.4.4.4
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 2
 neighbor 3.3.3.3 update-source Loopback0

 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family

 address-family ipv4 vrf BLUE
 redistribute connected
 no auto-summary
 no synchronization
 exit-address-family
 exit

no cdp run
```

Configuración CE2

CE2
hostname CE2 interface FastEthernet1/0 ip address 20.20.20.2 255.255.255.0 no shut exit interface FastEthernet0/0 ip address 172.16.4.1 255.255.255.0 no shut exit int fast 1/0 ip nat out exit int fast 0/0 ip nat ins exit ip route 0.0.0.0 0.0.0.0 20.20.20.254 ip nat inside source static 172.16.4.10 20.20.20.3 no cdp run

Modelo 3: MP-eBGP entre ASBRs - Redistribute connected

Configuración CE1

CE1
hostname CE1 interface Loopback0 ip address 99.99.99.99 255.255.255.255 int fa 1/0 no shut exit interface FastEthernet1/0.10 encapsulation dot1Q 10 ip address 10.10.10.1 255.255.255.0 exit router ospf 99 router-id 99.99.99.99 log-adjacency-changes network 99.99.99.99 0.0.0.0 area 0 network 10.10.10.0 0.0.0.255 area 0 exit

Configuración PE1

PE1
hostname PE1 no cdp run ip vrf R1 rd 1:1

```
 route-target export 1:1
 route-target import 1:1

 mpls label range 30 60
 mpls label protocol ldp

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 exit

int fa 1/0
 no shut
 exit

int fa 1/1
 no shut
 exit

interface FastEthernet1/0.10
 encapsulation dot1Q 10
 ip vrf forwarding R1
 ip address 10.10.10.254 255.255.255.0
 no shut
 exit

interface FastEthernet1/1.11
 encapsulation dot1Q 11
 ip address 11.11.11.1 255.255.255.0
 tag-switching ip
 mpls ip
 exit

router ospf 1
 router-id 1.1.1.1
 netw 11.11.11.0 0.0.0.255 area 3
 netw 1.1.1.1 0.0.0.0 are 3
 exit
router ospf 2 vrf R1
 log-adjacency-changes
 redistribute bgp 234 subnets
 network 10.10.10.0 0.0.0.255 area 0
 exit

router bgp 234
 bgp router-id 1.1.1.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 234
 neighbor 2.2.2.2 update-source Loopback0


 address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 exit-address-family

  address-family ipv4 vrf R1
 redistribute ospf 2 vrf R1 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 exit
```

Configuración P1-AS1

P1-AS1

```
hostname P1-AS1

no cdp run

mpls ldp router-id Loopback0
mpls label range 70 100
mpls label protocol ldp

interface Loopback0
 ip address 100.100.100.100 255.255.255.255
 exit

int fa 1/0
 no shut
 exit
interface FastEthernet1/0.11
 encapsulation dot1Q 11
 ip address 11.11.11.100 255.255.255.0
 mpls ip
 exit

int fa 1/1
 no shut
 exit

interface FastEthernet1/1.12
 encapsulation dot1Q 12
 ip address 12.12.12.100 255.255.255.0
 mpls ip
 exit
router ospf 100
 router-id 100.100.100.100
 netw 11.11.11.0 0.0.0.255 area 3
 netw 12.12.12.0 0.0.0.255 area 3
 netw 100.100.100.100 0.0.0.0 area 3
 exit
```

Configuración PE2

PE2

```
hostname PE2

mpls ldp router-id Loopback0
mpls label range 110 140
mpls label protocol ldp

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 exit

int fa 1/0
 no shut
 exit

int fa 1/1
 no shut
 exit
```

```
interface FastEthernet1/0.12
 encapsulation dot1Q 12
 ip address 12.12.12.2 255.255.255.0
 mpls ip
 exit

router ospf 2
 router-id 2.2.2.2
 netw 2.2.2.2 0.0.0.0 area 3
 netw 12.12.12.0 0.0.0.255 area 3
 exit

interface FastEthernet1/1.23
 encapsulation dot1Q 23
 ip address 23.23.23.2 255.255.255.0
 mpls bgp forwarding
 exit

router bgp 234
 bgp router-id 2.2.2.2
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 234
 neighbor 1.1.1.1 update-source Loopback0
  neighbor 23.23.23.3 remote-as 567

 address-family vpnv4
 neighbor 1.1.1.1 activate
 neighbor 1.1.1.1 next-hop-self
 neighbor 1.1.1.1 send-community extended
 neighbor 23.23.23.3 activate
 neighbor 23.23.23.3 send-community extended
 neighbor 23.23.23.3 route-map RT-REWRITE in
 exit-address-family
 exit

ip extcommunity-list 8 permit rt 8:8

route-map RT-REWRITE permit 10
 match extcommunity 8
 set extcomm-list 8 delete
 set extcommunity rt  1:1
 exit

route-map RT-REWRITE permit 1000
exit
```

Configuración PE3

PE3

```
hostname PE3

mpls ldp router-id Loopback0
mpls label range 30 60
mpls label protocol ldp

interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 exit
```

```
int fa 1/0
 no shut
 exit

int fa 1/1
 no shut
 exit

interface FastEthernet1/0.23
 encapsulation dot1Q 23
 ip address 23.23.23.3 255.255.255.0
 mpls bgp forwarding
 exit

interface FastEthernet1/1.32
 encapsulation dot1Q 32
 ip address 32.32.32.3 255.255.255.0
mpls ip
 exit

router ospf 3
 router-id 3.3.3.3
 netw 3.3.3.3 0.0.0.0 area 6
 netw 32.32.32.0 0.0.0.255 area 6
 exit

router bgp 567
 bgp router-id 3.3.3.3
  no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 567
 neighbor 4.4.4.4 update-source Loopback0
  neighbor 23.23.23.2 remote-as 234
 address-family vpnv4
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 next-hop-self
 neighbor 4.4.4.4 send-community extended
 neighbor 23.23.23.2 activate
 neighbor 23.23.23.2 send-community extended
 neighbor 23.23.23.2 route-map RT-REWRITE in
 exit-address-family
 exit

ip extcommunity-list 1 permit rt 1:1

route-map RT-REWRITE permit 10
 match extcommunity 1
 set extcomm-list 1 delete
 set extcommunity rt  8:8
 exit

route-map RT-REWRITE permit 1000
 exit
```

Configuración P1-AS2

P1-AS2
hostname P1-AS2 mpls ldp router-id Loopback0

```
mpls label range 70 100
mpls label protocol ldp

interface Loopback0
 ip address 200.200.200.200 255.255.255.255
 exit

int fa 1/0
 no shut
 exit

int fa1/1
 no shut
 exit

interface FastEthernet1/0.32
 encapsulation dot1Q 32
 ip address 32.32.32.200 255.255.255.0
 mpls ip
 exit

interface FastEthernet1/1.24
 encapsulation dot1Q 24
 ip address 24.24.24.200 255.255.255.0
 mpls ip
 exit
 router ospf 200
 router-id 200.200.200.200
 netw 200.200.200.200 0.0.0.0 area 6
 netw 32.32.32.0 0.0.0.255 area 6
 netw 24.24.24.0 0.0.0.255 area 6
 exit
```

Configuración PE4

PE4

```
hostname PE4

ip vrf R8
 rd 8:8
 route-target export 8:8
 route-target import 8:8
 exit

mpls label range 110 140
mpls label protocol ldp
tag-switching tdp router-id Loopback0

interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 exit

int fa 1/0
 no shut
 exit

int fa 1/1
 no shut
 exit

interface FastEthernet1/0.24
```

```
 encapsulation dot1Q 24
 ip address 24.24.24.4 255.255.255.0
 tag-switching ip
 exit

interface FastEthernet1/1.20
 encapsulation dot1Q 20
 ip vrf forwarding R8
 ip address 20.20.20.254 255.255.255.0
 exit

router ospf 4
 router-id 4.4.4.4
 netw 4.4.4.4 0.0.0.0 area 6
 netw 24.24.24.0 0.0.0.255 area 6
 exit

router ospf 7 vrf R8
 log-adjacency-changes
 redistribute bgp 567 subnets
 network 20.20.20.0 0.0.0.255 area 0
 exit

router bgp 567
 bgp router-id 4.4.4.4
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 567
 neighbor 3.3.3.3 update-source Loopback0

 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family

  address-family ipv4 vrf R8
 redistribute ospf 7 vrf R8 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 exit
```

Configuración CE2

CE2

```
hostname CE2

interface Loopback0
 ip address 88.88.88.88 255.255.255.255
 exit

interface FastEthernet1/0.20
 encapsulation dot1Q 20
 ip address 20.20.20.2 255.255.255.0
 exit

int fast 1/0
 no shut
 exit

router ospf 88
```

```
router-id 88.88.88.88
log-adjacency-changes
network 88.88.88.88 0.0.0.0 area 0
 network 20.20.20.0 0.0.0.255 area 0
exit
```

Modelo 4: Multihop MP-eBGP entre Route-Reflectors (RRs)

Configuración CE1

CE1

```
hostname CE1

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet 1/0.12
 encapsulation dot1Q 12
 ip address 12.12.12.1 255.255.255.0
 exit

router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 12.12.12.1 0.0.0.0 area 0
 exit
```

Configuración PE1

PE1

```
host PE1

no cdp run

ip vrf CE1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 exit

mpls label range 30 60
mpls label protocol ldp

tag-switching tdp router-id Loopback0

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

int fast 1/1
 no shut
```

```
 exit

 interface FastEthernet1/0.12
  encapsulation dot1Q 12
  ip vrf forwarding CE1
  ip address 12.12.12.2 255.255.255.0
  exit

 interface FastEthernet1/1.23
  encapsulation dot1Q 23
  ip address 23.23.23.2 255.255.255.0
  mpls ip
  exit

 router ospf 2 vrf CE1
  log-adjacency-changes
  redistribute bgp 234 subnets
  network 12.12.12.2 0.0.0.0 area 0
  exit

 router ospf 10
  router-id 2.2.2.2
  netw 23.23.23.0 0.0.0.255 area 3
  netw 2.2.2.2 0.0.0.0 area 3
  exit
 router bgp 234
  bgp router-id 2.2.2.2
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 3.3.3.3 remote-as 234
  neighbor 3.3.3.3 update-source Loopback0

  address-family ipv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-label
  no auto-summary
  no synchronization
  network 2.2.2.2 mask 255.255.255.255
  exit-address-family

  address-family vpnv4
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
  exit-address-family

  address-family ipv4 vrf CE1
  redistribute ospf 2 vrf CE1 match internal external 1 external 2
  no auto-summary
  no synchronization
  exit-address-family
 exit
```

Configuración P1-AS1

P1-AS1
host P1-AS1 no cdp run mpls label range 70 100

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/1
 no shut
 exit

interface FastEthernet1/0.23
 encapsulation dot1Q 23
 ip address 23.23.23.3 255.255.255.0
 mpls ip
 exit

interface FastEthernet1/1.34
 encapsulation dot1Q 34
 ip address 34.34.34.3 255.255.255.0
 mpls ip
 exit

router ospf 20
 router-id 3.3.3.3
 netw 3.3.3.3 0.0.0.0 area 3
 netw 23.23.23.0 0.0.0.255 area 3
 netw 34.34.34.0 0.0.0.255 area 3
 exit

router bgp 234
 bgp router-id 3.3.3.3
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 234
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 4.4.4.4 remote-as 234
 neighbor 4.4.4.4 update-source Loopback0
 neighbor 6.6.6.6 remote-as 567
 neighbor 6.6.6.6 ebgp-multihop 255
 neighbor 6.6.6.6 update-source Loopback0

 address-family ipv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 route-reflector-client
 neighbor 2.2.2.2 send-label
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 route-reflector-client
 neighbor 4.4.4.4 send-label
 no auto-summary
 no synchronization
 network 3.3.3.3 mask 255.255.255.255
 exit-address-family

 address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 route-reflector-client
 neighbor 2.2.2.2 send-community extended
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 next-hop-unchanged
 neighbor 6.6.6.6 send-community extended
```

```
 neighbor 6.6.6.6 route-map RT-REWRITE in
 exit-address-family

ip extcommunity-list 8 permit rt 8:8

route-map RT-REWRITE permit 10
 match extcommunity 8
 set extcomm-list 8 delete
 set extcommunity rt  1:1

route-map RT-REWRITE permit 1000
```

Configuración PE2

PE2

```
host PE2
no cdp run
mpls ldp router-id Loopback0
mpls label range 110 140
mpls label protocol ldp

interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/1
 no shut
 exit

interface FastEthernet1/0.34
 encapsulation dot1Q 34
 ip address 34.34.34.4 255.255.255.0
 mpls ip
 exit

interface FastEthernet1/1.45
 encapsulation dot1Q 45
 ip address 45.45.45.4 255.255.255.0
 mpls bgp forwarding
 exit

router ospf 30
 router-id 4.4.4.4
 netw 4.4.4.4 0.0.0.0 area 3
 netw 34.34.34.0 0.0.0.255 area 3
 exit

router bgp 234
 bgp router-id 4.4.4.4
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 234
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 45.45.45.5 remote-as 567

 address-family ipv4
 neighbor 3.3.3.3 activate
```

```
 neighbor 3.3.3.3 next-hop-self
 neighbor 3.3.3.3 send-label
 neighbor 45.45.45.5 activate
 neighbor 45.45.45.5 send-label
 no auto-summary
 no synchronization
 exit-address-family
```

Configuración PE3

PE3

```
host PE3
no cdp run

mpls ldp router-id Loopback0
mpls label range 30 60
mpls label protocol ldp

interface Loopback0
 ip address 5.5.5.5 255.255.255.255
 exit
interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/1
 no shut
 exit

interface FastEthernet1/0.45
 encapsulation dot1Q 45
 ip address 45.45.45.5 255.255.255.0
 mpls bgp forwarding
 exit

interface FastEthernet1/1.56
 encapsulation dot1Q 56
 ip address 56.56.56.5 255.255.255.0
 mpls ip
  exit

router ospf 40
 router-id 5.5.5.5
 netw 5.5.5.5 0.0.0.0 area 2
 netw 56.56.56.0 0.0.0.255 area 2
 exit

router bgp 567
 bgp router-id 5.5.5.5
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 6.6.6.6 remote-as 567
 neighbor 6.6.6.6 update-source Loopback0
 neighbor 45.45.45.4 remote-as 234

  address-family ipv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 next-hop-self
 neighbor 6.6.6.6 send-label
 neighbor 45.45.45.4 activate
 neighbor 45.45.45.4 send-label
```

```
no auto-summary
no synchronization
exit-address-family
```

Configuración P1-AS2

P1-AS2

```
host P1-AS2
no cdp run

interface Loopback0
 ip address 6.6.6.6 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/1
 no shut
 exit

interface FastEthernet1/0.56
 encapsulation dot1Q 56
 ip address 56.56.56.6 255.255.255.0
 mpls ip
 exit

interface FastEthernet1/1.67
 encapsulation dot1Q 67
 ip address 67.67.67.6 255.255.255.0
 mpls ip
 exit

router ospf 50
 router-id 6.6.6.6
 netw 6.6.6.6 0.0.0.0 area 2
 netw 56.56.56.0 0.0.0.255 area 2
 netw 67.67.67.0 0.0.0.255 area 2
 exit

router bgp 567
 bgp router-id 6.6.6.6
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 234
 neighbor 3.3.3.3 ebgp-multihop 255
 neighbor 3.3.3.3 update-source Loopback0
 neighbor 5.5.5.5 remote-as 567
 neighbor 5.5.5.5 update-source Loopback0
 neighbor 7.7.7.7 remote-as 567
 neighbor 7.7.7.7 update-source Loopback0

 address-family ipv4
 neighbor 5.5.5.5 activate
 neighbor 5.5.5.5 route-reflector-client
 neighbor 5.5.5.5 send-label
 neighbor 7.7.7.7 activate
 neighbor 7.7.7.7 route-reflector-client
 neighbor 7.7.7.7 send-label
 no auto-summary
```

```
 no synchronization
 network 6.6.6.6 mask 255.255.255.255
 exit-address-family

 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 next-hop-unchanged
 neighbor 3.3.3.3 send-community extended
 neighbor 3.3.3.3 route-map RT-REWRITE in
 neighbor 7.7.7.7 activate
 neighbor 7.7.7.7 route-reflector-client
 neighbor 7.7.7.7 send-community extended
 exit-address-family
ip extcommunity-list 1 permit rt 1:1

route-map RT-REWRITE permit 10
 match extcommunity 1
 set extcomm-list 1 delete
 set extcommunity rt  8:8
 exit

route-map RT-REWRITE permit 1000
```

Configuración PE4

PE4

```
host PE4

ip vrf CE2
 rd 8:8
 route-target export 8:8
 route-target import 8:8
 exit

mpls label range 110 140
mpls label protocol ldp
tag-switching tdp router-id Loopback0

interface Loopback0
 ip address 7.7.7.7 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/1
 no shut
 exit

interface FastEthernet1/0.67
 encapsulation dot1Q 67
 ip address 67.67.67.7 255.255.255.0
 mpls ip
 exit

interface FastEthernet1/1.78
 encapsulation dot1Q 78
 ip vrf forwarding CE2
 ip address 78.78.78.7 255.255.255.0
 exit
```

```
router ospf 7 vrf CE2
 log-adjacency-changes
 redistribute bgp 567 subnets
 network 78.78.78.7 0.0.0.0 area 0
 exit

router ospf 60
 router-id 7.7.7.7
 netw 7.7.7.7 0.0.0.0 area 2
 netw 67.67.67.0 0.0.0.255 area 2
 exit
router bgp 567
 bgp router-id 7.7.7.7
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 6.6.6.6 remote-as 567
 neighbor 6.6.6.6 update-source Loopback0

 address-family ipv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 send-label
 no auto-summary
 no synchronization
 network 7.7.7.7 mask 255.255.255.255
 exit-address-family

 address-family vpnv4
 neighbor 6.6.6.6 activate
 neighbor 6.6.6.6 send-community extended
 exit-address-family

 address-family ipv4 vrf CE2
 redistribute ospf 7 vrf CE2 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 exit
```

Configuración CE2

CE2

```
hostname CE2
no cdp run
interface Loopback0
 ip address 8.8.8.8 255.255.255.255
 exit

interface FastEthernet1/0
 no shut
 exit

interface FastEthernet1/0.78
 encapsulation dot1Q 78
 ip address 78.78.78.8 255.255.255.0
 exit
router ospf 8
 router-id 8.8.8.8
 log-adjacency-changes
 network 8.8.8.8 0.0.0.0 area 0
 network 78.78.78.8 0.0.0.0 area 0
 exit
```